www.optenet.com

OPTENET WEB FILTER Server 5.27
Windows/Linux/Solaris/Aix/MacOS

User's Manual

Rev 28-06-2006

INDEX

1. INTRODUCTION 5

2. NEW CHARACTERISTICS OF VERSION 5.27 6

3. INSTALLATION 7

3.1. SYSTEM REQUIREMENTS 7
3.2. INSTALLATION 8
3.3. START-UP AND SHUT DOWN 24
3.4. AUTOMATIC STARTING AND STOPPING WITH THE SYSTEM 27
3.5. CONFIGURATION OF A BLUECOAT APPLIANCE SO THAT IT USES OPTENET AS A FILTERING SYSTEM (ICAP) 28
3.6. CONFIGURING NETCACHE TO USE OPTENET AS THE FILTERING SYSTEM 34

4. BASIC CONCEPTS 38

4.1. USER 38
4.2. GROUP 38
4.3. IP ADDRESS 38
4.4. URL 39
4.5. CATEGORY 39
4.6. RULE 40

5. ADMINISTRATION 41

5.1. INTRODUCTION 41
5.2. DOCUMENTATION 43
5.3. CONFIGURATION 43
5.4. AUTHENTICATION 47
5.5. CATEGORIES 58
5.6. URL CLASSIFICATION 59
5.7. FILTERING RULES 62
5.8. UPDATES 71
5.9. REPORTS 73
5.10. ADMINISTRATOR IDENTIFICATION 74
5.11. ADVANCED CONFIGURATION 75
5.12. CLUSTER MANAGEMENT 80
5.13. LICENSE 87
5.14. SYSTEM INFORMATION 87

6. FREQUENT PROBLEMS 89

6.1. THE OPTENET SERVER ERROR MESSAGE... APPEARS WHEN I TRY TO SURF 89
6.2. THE FILTER WILL NOT START 89
6.3. THE USERS DO NOT APPEAR WHEN THE REFRESH BUTTON IS PRESSED 90
6.4. I CANNOT ENTER THE FILTER ADMINISTRATION 90
6.5. DEP CLOSES OPTENET SERVER IN W2003 SP1 90

ANNEX 93

1. ADMINISTRATION OF OPTENET SERVER TROUGH A SECURE CONNECTION (ONLY LINUX ENVIRONMENT) 94

2. ADMINISTRATION OF OPTENET VIA THE COMMAND LINE (OPTENET CLI V1.0) 95

2.1. INTRODUCTION 95
2.2. USE 95
2.3. COMMAND REFERENCES 98
2.4. MOST COMMON PROBLEMS 106

3. OPTENET PROXY CONFIGURATION 107

3.1. CONFIGURING A CHAINED PROXY (CONFIGURATION PROXY) 107
3.2. OPTENET SERVER ADMINISTRATION 107
3.3. PORT CONFIGURATION (PORT PROXY) 108

4. DESCRIPTION OF OPTENET CATEGORIES 108

5. ICAP NOW 112

6. SNMP MONITORING (ONLY LINUX ENVIRONMENT) 114

6.1. EXECUTING THE SNMP AGENT 114
6.2. AUTOMATIC START 115
6.3. CONFIGURATION OF THE AGENT 115

7. ADVANCED CGIS CONFIGURATION 115

7.1. RELOAD 115
7.2. DUMPING OF LOGS ONTO DISKS (/CGI-BIN/FLUSHLOGS) 115
7.3. SYSTEM INFORMATION IN TEXT MODE (/CGI-BIN/SYSINFOTXT) 116

8. CONFIGURING MICROSOFT ISA 2004 116

8.1. INTRODUCTION 116
8.2. ACCESS TO OPTENET'S LICENCE AND UPDATES SERVERS 116
8.3. ACCESS TO THE DEFAULT BLOCKING PAGE 119

1. INTRODUCTION

OPTENET is a filtering system that enables a company's Internet resources and the time used on the Internet to be optimised. By installing it on the server that provides your network connection you will be able to filter the Internet pages that you consider inappropriate and monitor the user access.

In order to carry out the filtering, OPTENET Server must always work with a proxy. The proxy guarantees that all the network web requests go through it, therefore, OPTENET Server only has to be joined to the proxy in order to filter the whole network. If the network to be filtered has computers whose web requests do not go through the proxy they will not be filtered. The process by which OPTENET communicates with the proxy is using an extension (or ***plug in)*** or using an ICAP client if the proxy supports this protocol. When a user tries to access a page web he or she requests the page from the proxy. When the request reaches the proxy it is captured by OPTENET Server ***plug in*** which decides if the request should be allowed or not.

To make this decision the OPTENET Server service is based on a set of rules that the administrator defines according to the following criteria:

Page requested (URL, file type or content type).
User that makes the request (names and IP address) and group(s) to whom he/she belongs.
The time the request is made (day of the week and time).
Type of files (music, video, exe, etc.).
And it also offers the possibility to manually define the lists of URLs which will be used to allow or block access.

If the set of rules establishes that the requested page should be allowed the page is shown as is on the user's browser. However, if it is decided that the request should be denied, the user is shown another page that informs about the block carried out. In turn this block is registered for possible monitoring of the network use.

The main characteristic of OPTENET Server consists of the categorisation of contents that are offered by the system. Through the combination of a database of previously classified URLs and a multilingual content analyser OPTENET Server is able to classify the web pages in several categories that can be combined when defining the filtering rules.

OPTENET Server 5.20f can work as an ICAP server integrated with all appliances or caches that support this protocol (on Windows, Linux, Solaris or Aix), it can also be installed with the SQUID 2.5 proxy on Linux, Solaris and Aix or it can be installed with Microsoft ISA proxy, Microsoft Proxy Server or the OPTENET proxy in Windows environments. Its leading technology in the selection and filtering of Internet access will allow the greatest control of the use of the Internet of all of the workstations connected to the network.

To manage the access to the Internet, OPTENET has four filtering levels:

- Filtering according to the **multilingual semantic analysis of the text** that appears on the web page. OPTENET analyses each page **at the moment it is downloaded** from the Internet, thereby allowing a greater security level.
- Filtering based on **predefined lists** with addresses classified manually by specialists.
- Filtering based on **URL analysis.**

- Filtering based on **lists predefined by the actual users.**

In addition, OPTENET Server offers the following features:
- Automatic updating of lists.
- Personalisation of the predefined lists.
- Multi-language web based administration (English, French, Spanish, Italian and Portuguese).

2. NEW CHARACTERISTICS OF VERSION 5.27

These are the new features and improvements of version 5.27 with respect to its predecessor 5.25:

- Added categories: Street maps and guides, Art and culture, Info, Legal, Banks and financial institutions, Blogs, Pay to surf, Logos/ringtones, Malware, DNS services, Telecommunications.
- Possibility of working with ICAP and ISA on LDAP when a user identifier is employed other than "**Distinguished name**".
- Skype protocol filtering (when this is integrated with ICAP)
- User identification using digital certificates, when LDAP authentication is used.
- It is possible to enquire through the web administrator to which categories a specific URL belongs.
- It is possible to apply filtering rules to those requests that to not fall into any of the categories supported by the filtering tool.

3. INSTALLATION

This section describes the installation of OPTENET and the necessary requirements of the Windows, Linux o Solaris system where OPTENET is going to be installed.

3.1. System requirements

3.1.1. On Windows systems

- Microsoft Windows 98/Me/NT/2000/ XP/2003
- OPTENET recommends using Windows Server systems (NT/2000/2003) due to the greater stability available. The filter is also easier to manage as it can be installed as an easily restarted and stopped service.
  Latest Windows Service Pack recommended.
- The equipment depends on the number of users, but a CPU with at least 266 MHz and 128 Mbytes of RAM is recommended.

3.1.2. On Linux systems

- Kernel Linux 2.0 or later.
- Glibc 2.0.7 or later, given its thread support.
- Portmap service, required for the RPC communication (if it is installed to work with SQUID).
- Red Hat Linux version 7.0 or later is recommended.
- The minimum equipment logically depends on the number of users, but a CPU of at least 266 MHz and 128 Mbytes of RAM memory is recommended.

3.1.3. On Solaris systems

- Solaris 2.6 or later version.
- Rpcbind service, required for the RPC communication (if it is installed to work with SQUID).
- The equipment depends on the number of users, but a Sun UltraSPARC with at least 200 MHz and 128 Mbytes of RAM is recommended.

3.1.4. On Aix systems

- Aix 4.3
- portmap service for RPC communication.
- The machine used depends on the number of users, but a minimum recommendation is a PowerPC running at 200MHz with 128 Mbytes of RAM.
- GNU tar and gzip.
- gcc 3.2.1 Aix runtime libraries.

3.1.5. Under Mac OS X

- Mac OS X 10.3.3 or later.
- Portmap service for RPC communication (already included in Mac OS X).

- The equipment involved depends on the number of users. However, it is recommended that a G4 processor and 256 MB of RAM be used.

3.2. Installation

In order to carry out the filtering, OPTENET Server must always work with a proxy. The proxy centralises all user web access, therefore, OPTENET Server only has to be joined to the proxy in order to filter the whole network. If the network to be filtered has computers whose web requests do not go through the proxy they will not be filtered.

OPTENET Server allows its own Proxy to be installed under Windows, which is suitable to give service for networks of up to 200 users. Under Unix (Linux, Solaris, Aiz, MacOS) the Proxy SQUID is distributed, capable of giving service to medium and large networks.

In addition, at the end of the installation of OPTENET Server, you are given the opportunity to install OPTENET Reporter, a tool that enables the creation of reports on Internet use.

3.2.1. On Windows systems

To install OPTENET Server on your server run the OPTENET-5.27.XX-2.03.XX.exe program (or later version). If it is not one of the 3 available languages, English is selected.

This program includes OPTENET Server and OPTENET Reporter. Once the installation of OPTENET Server is complete, the opportunity is given to install OPTENET Reporter.

This program can be used to install just one of the two products. For more information on OPTENET Reporter (installation, configuration…), check the corresponding manual.

The process for installing OPTENET Server only is detailed below.

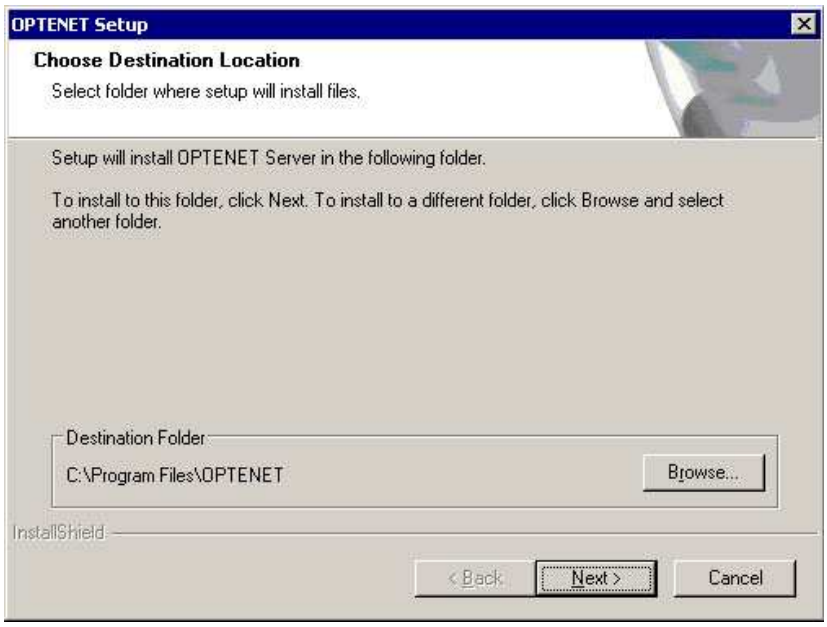
A window is than displayed asking if you want to install OPTENET Server. Answer yes.

Below you must select the type of installation you want:

- Demo: installation with temporary license. It is the default installation you do not need to introduce any license number. The time limit is activated from the moment of installation, not from the moment of downloading. This Demo license will be valid for 30 days.
- Paying: indefinite installation. Select this option and then introduce your valid license code.

If you want an indefinite installation, but do not have your licence code yet, install it using the ‘demo’ mode, as you can introduce the licence code at any time from the OPTENET Server administration.

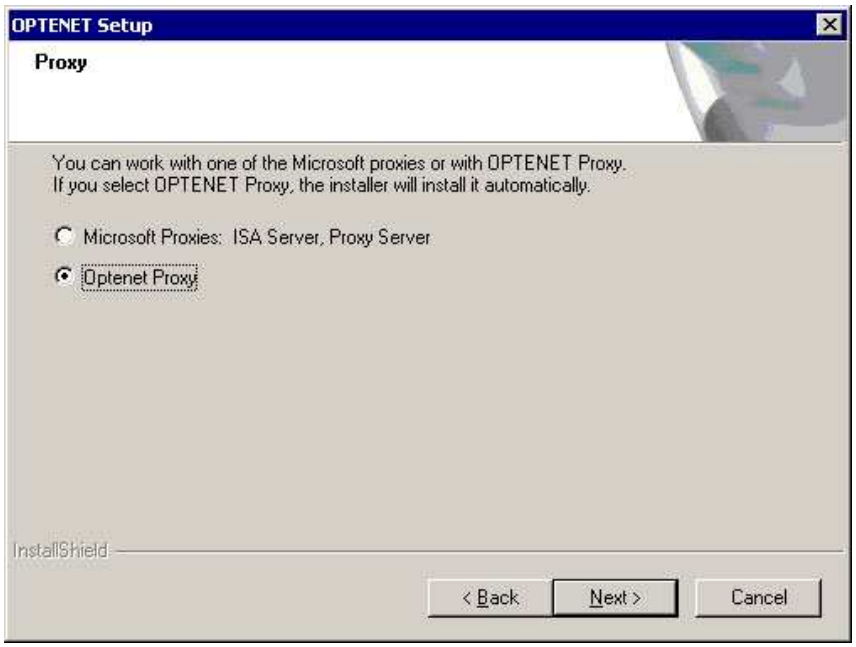
You will then be asked for the software installation directory . The default directory is C:\Program files\OPTENET but you can select any other one. If the chosen directory does not exist the installation program will create it.


OPTENET Setup
Choose Destination Location
Select folder where setup will install files.
Setup will install OPTENET Server in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files\OPTENET
Browse...
InstallShield
< Back
Next >
Cancel

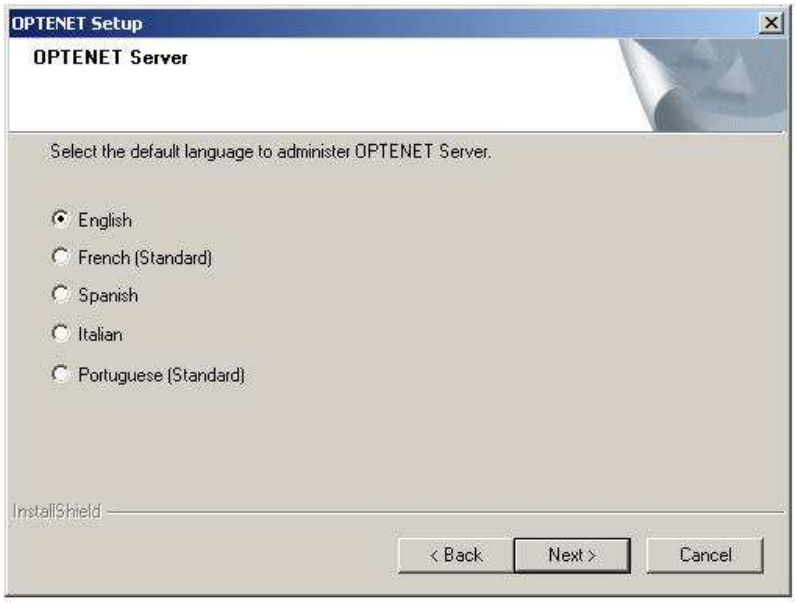
Clicking on next will allow you to select the communications protocol that the OPTENET server should use to communicate with the proxy. The proxies that can use the protocol is shown

OPTENET Setup
OPTENET Server <-> Proxy
For each protocol, the proxies that OPTENET Server can work with are shown. In accordance with your proxy, select the associated protocol.
RPC: ISA, MS Proxy, OPTENET Proxy
NetScreen CSP
ICAP: NetCache, CacheFlow
PIX
Border Manager
CheckPoint UFP
InstallShield
< Back
Next >
Cancel

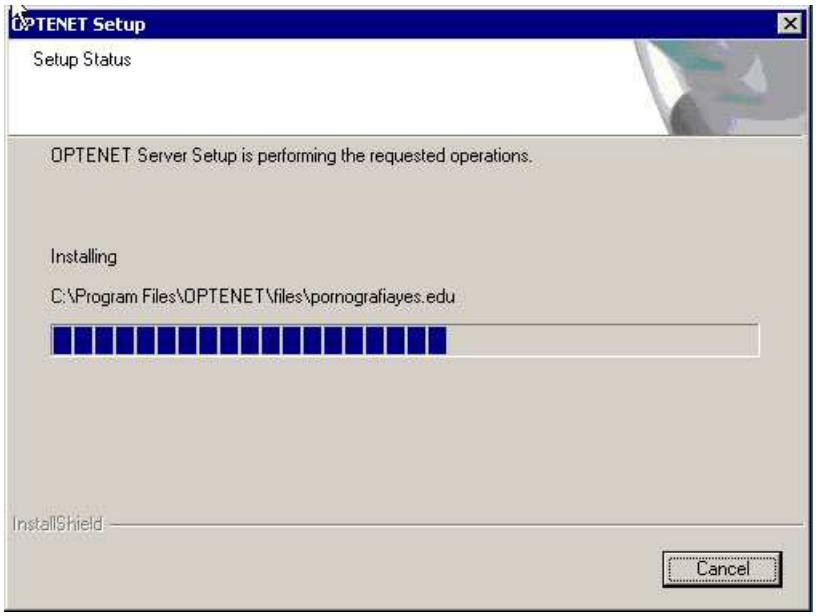
If you have selected RPC on the previous screen you can now configure OPTENET server to work with a Microsoft proxy (ISA Server, MS Proxy Server) or with the OPTENET proxy:


OPTENET Setup
Proxy
You can work with one of the Microsoft proxies or with OPTENET Proxy.
If you select OPTENET Proxy, the installer will install it automatically.
Microsoft Proxies: ISA Server, Proxy Server
Optenet Proxy
InstallShield
< Back
Next >
Cancel

Next, select the default web based administration language: (Administration, web, Report tools, logs etc.).



Click on Next and the installer will install and configure OPTENET Server. The server will be running the next time you restart the machine.



Finally you will be asked if you want to install OPTENET Reporter. If you do not wish to, you will be asked to restart the computer. OPTENET Server will not run correctly until the machine has been restarted.

Group of programs

OPTENET Server creates a new Program group with its most characteristic elements.

- **Contribution:** This option allows you to add webs to the filter.
- **Uninstall OPTENET Server:** This element uninstalls OPTENET Server from your server.
- **Administration:** If you select this element your browser will be opened and you will be connected to the OPTENET Server WWW Administration.
- **www.optenet.com:** If you select this element your browser will be opened and you will be connected to the OPTENET web page: http://www.optenet.com.
- **WWW User manual:** This element will enable you to access the latest online version of the OPTENET Server manual.

Windows REGISTRY

For the correct operation of OPTENET Server the installation program carries out a series of modifications in the Windows Registry.

To save the basic parameters of OPTENET Server the installation program adds the key HKEY_LOCAL_MACHINE\SOFTWARE\OPTENET\OPTENET Server\

CheckData If you have installed OPTENET server along with a Microsoft Proxy and additionally have an antivirus working as an ISAPI plug in for this proxy this value should be set to FALSE. For all other cases this value (the default value) should be TRUE.

DownloadContent Flag that indicates to OPTENET Server whether it must request the content when it is integrated with PIX, Border Manager and CheckPoint. By default "TRUE", i.e. it requests content.
FilterServer Server where OPTENET Server service is run and where the OPTENET Server plug in should send the data. The default value is 127.0.0.1 (localhost)
IcapClients It identifies the number of icap clients when being integrated with an ICAP server. (NetCache, BlueCoat). By default 1.
IcapPort ICAP Server listening port. The default port is 1344.
InstallDir OPTENET Server installation Directory.
Language OPTENET Server language identifier and which is selected during the installation process. (eng, esp, fra, ita, por)
ManagerPort Listening port of the OPTENET WWW Administration server. The default port is 10237.
Mode The communications mode between the OPTENET server and the proxy. Two values are used: RPC and ICAP.
Proxy Identifies the proxy with which OPTENET Server is integrated (ICA, PIX, BMA, OPT, MSP, UFP).
RemoveDomain Flag that indicates to OPTENET Server as a user and group identifier. with its name ("TRUE" by default) or using the domain name in front ("FALSE", i.e. namedomain\username).
Version It identifies the version of OPTENET Server currently installed.
SendIpUser This indicates to OPTENET Server whether it must send the client's user and ip as stop page parameters to the client in question whose page has stopped. By defect its value is FALSE.
LogServerPort OPTENET Server's listening port for requests for the logs made by OPTENET Reporter. The default port is 10239.
LogServerClients Number of threads launched by OPTENET Server to meet the requests for logs made by OPTENET Reporter. By default it is 5.
WebserverThreads Number of threads OPTENET Server will launch in order to cater for administration requests. By default, 50.
BindIpLocal Local ip address (network interface) on which OPTENET Server listens. By default 0.0.0.0 (all network interfaces). This parameter is useful when there are various network interfaces and we do not wish OPTENET Server to listen to all of them.
DiscardHeaders Headers that the OPTENET Server for ISA should ignore. The header 'X-Actual-URL' needs to be added if RealPlayer traffic goes through Microsoft ISA. Should more than one header be added, they should be separated by commas.

To save the basic parameters of OPTENET Reporter, the installation process adds the key HKEY LOCAL MACHINE\SOFTWARE\OPTENET\OPTENET Reporter.
InstallDir Installation directory of OPTENET Server**.**

System data

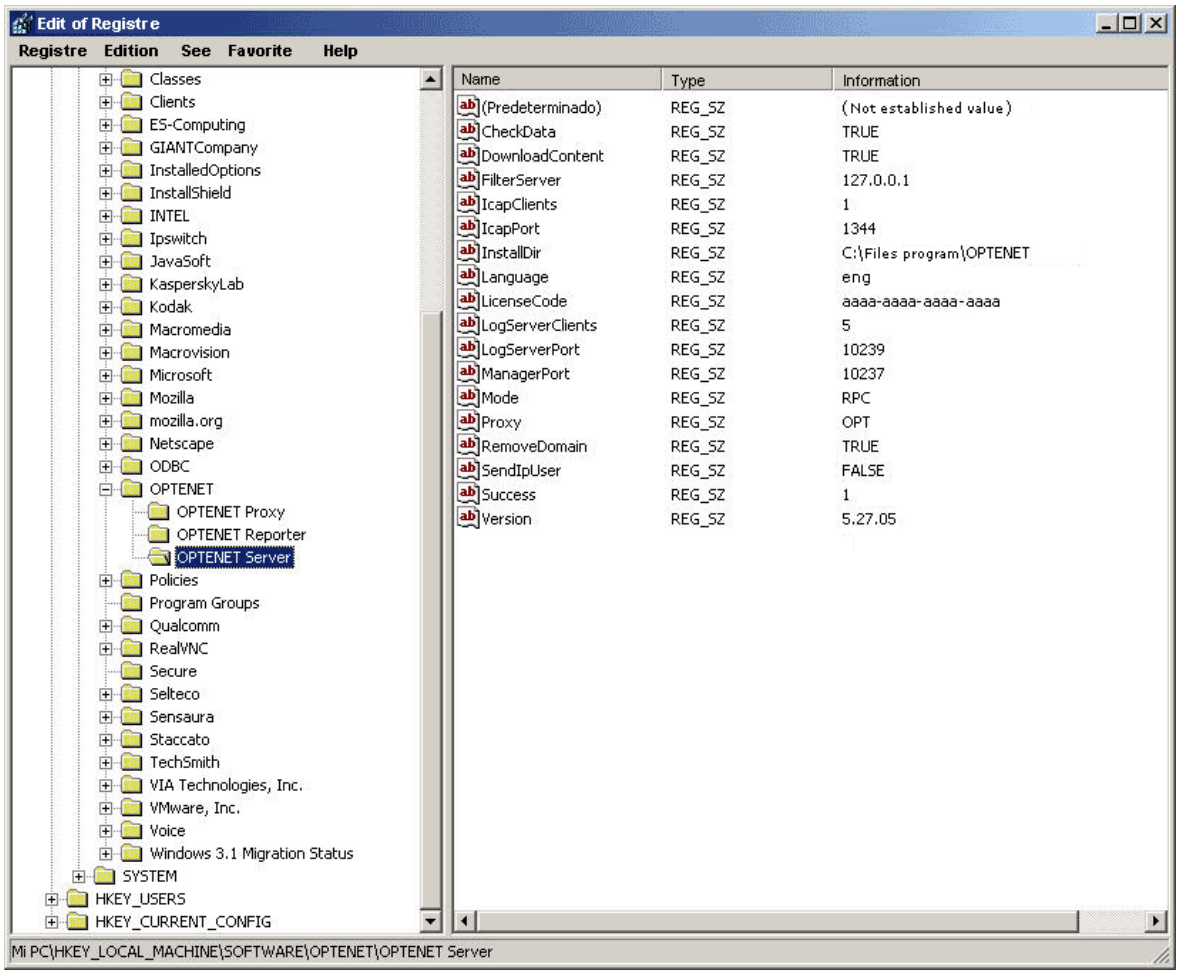
In order for OPTENET Server, OPTENET Reporter and OPTENET Proxy to be executed as a Windows service, use the Events viewer and uninstall it correctly, the OPTENET installation process adds a series of keys in the system data that are stored in the Windows Logs:

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OPTENET.**
The data required so that OPTENET Server can be executed as a service. In Windows 98 and Me this value is not used.

- **HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\OPTENET Proxy** The data required so that OPTENET proxy can be executed as a service. In Windows 98 and Me this register entry is not added as there is no service.

- **HKEY_LOCAL_MACHINE\SYSTEM\ Current ControlSet\Services_ _Eventlogn\Application\OPTENET.** The data required so that OPTENET Server can use the Events viewer to inform about problems.

- **HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current Version\ Uninstall\OPTENET Server**. The necessary data so that OPTENET Server can be uninstalled correctly.



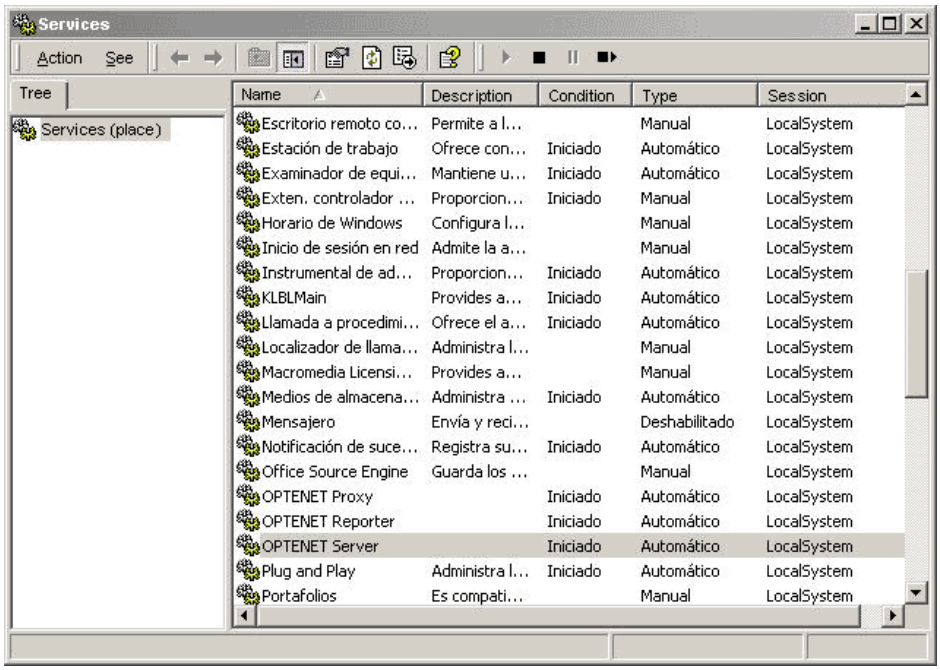
OPTENET Server Elements

The elements installed as OPTENET Server are divided into two main parts: one that is in charge of capturing requests from the Internet, and the other that manages the filtering of these requests.

The first element depends on the proxy that is used. This matter is covered in detail in the following sections.

The second element of OPTENET Server is a Windows service/process that analyses the requests that are received from OPTENET Server plug in installed with a proxy or as an ICAP client to the proxy and decides if these requests should be allowed or not. If the server has been installed as a service (NT, XP, 2000, 2003) you can see if it has been installed correctly in the Windows Services

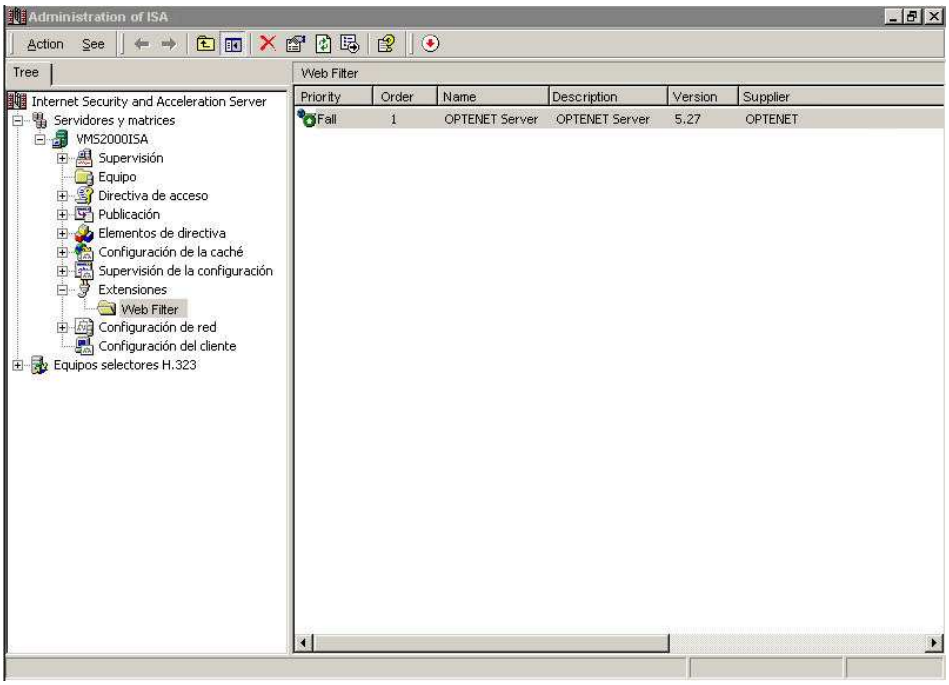
The same check can be performed for OPTENET Reporter and OPTENET Proxy.


Services
Action
See
Tree
Services (place)
Name
Description
Condition
Type
Session
Escritorio remoto co... Permite a l... Manual LocalSystem
Estación de trabajo Ofrece con... Iniciado Automático LocalSystem
Examinador de equi... Mantiene u... Iniciado Automático LocalSystem
Exten. controlador ... Proporcion... Iniciado Manual LocalSystem
Horario de Windows Configura l... Manual LocalSystem
Inicio de sesión en red Admite la a... Manual LocalSystem
Instrumental de ad... Proporcion... Iniciado Automático LocalSystem
KLBLMain Provides a... Iniciado Automático LocalSystem
Llamada a procedimi... Ofrece el a... Iniciado Automático LocalSystem
Localizador de llama... Administra l... Manual LocalSystem
Macromedia Licensi... Provides a... Manual LocalSystem
Medios de almacena... Administra ... Iniciado Automático LocalSystem
Mensajero Envía y reci... Deshabilitado LocalSystem
Notificación de suce... Registra su... Iniciado Automático LocalSystem
Office Source Engine Guarda los ... Manual LocalSystem
OPTENET Proxy Iniciado Automático LocalSystem
OPTENET Reporter Iniciado Automático LocalSystem
OPTENET Server Iniciado Automático LocalSystem
Plug and Play Administra l... Iniciado Automático LocalSystem
Portafolios Es compati... Manual LocalSystem

3.2.1.1. Integration with Microsoft ISA-Server proxy

The element in charge of capturing the requests is the OPTENET **plugin**, as already mentioned in the Introduction. It is a Web Filter that is added to Microsoft ISA Server. You can see if it has been installed correctly from the ISA server's Administration.

If OPTENET Server is integrated with Microsoft ISA 2004 please see Appendix 8 Configuring Microsoft ISA 2004 once OPTENET Server has been installed.



Microsoft Web Proxy

Microsoft Web Proxy is the proxy that is installed with Microsoft ISA Server. It is a Windows service and therefore it can be managed via the Windows services administration. OPTENET Server works closely with Microsoft Web Proxy: it can only filter the requests that go through the proxy.

Therefore, if you have Microsoft ISA Server installed but you do not use Microsoft Web Proxy, OPTENET Server will not carry out any kind of filtering. The most common way to ensure that computers use Microsoft Web Proxy is to configure their browsers for this purpose. You can **consult the Microsoft ISA Server documentation** to establish a **browser as a client of Microsoft Web Proxy**.

If you do not wish to configure the browsers for use with Microsoft Web Proxy but you use Microsoft ISA Server as Secure Server or SecureNAT Server on your network, you can link the Secure Server and Microsoft Web Proxy SecureNAT Server via the HTTP redirecting Filter. This way you will also ensure that the web requests go through Microsoft Web Proxy and they can be filtered by OPTENET Server. You can **consult the Microsoft ISA Server documentation** to obtain more information about this option.

Communication between Microsoft Web Proxy and OPTENET Server

In order for the requests that go through Microsoft Web Proxy to be filtered, OPTENET Server adds a Web Filter to Microsoft ISA Server . This Web filter consists of a Microsoft Web Proxy plugin that is in charge of capturing the data from the requests that go through it and sending them to the OPTENET Server filtering service. **The captured data is as follows:**

- The **IP address** of the computer the request comes from.
- The **user** that makes the request (only if Microsoft Web Proxy carries out the authentication).
- The **URL** of the requested page.
- **The content of the requested page**.

With this data the OPTENET Server service checks the filtering rules that are configured and decides if the request should be allowed or not. Depending on the result, it informs the plug in whether it should allow the request to continue along the usual path or it should block it. In the event of a block OPTENET Server service indicates the blocking page the plug in should show instead of the requested page.

The communication between the plug in and OPTENET Server service is carried out via remote procedure calls (RPC) and therefore the RPC service must be started.

3.2.1.2. Integration with Microsoft Proxy Server

For OPTENET Server to work correctly with a Microsoft Proxy Server, the Proxy Server should be installed using the following Microsoft recommendations:

1. Install Microsoft Windows NT 4.0 Service Pack 3 (Not Windows NT 4.0 Service Pack 4 or later).
2. Install Microsoft Internet Explorer 4.01 Service Pack 2 without the Active Desktop interface.

   NOTE: Windows NT Option Pack contains Internet Explorer 4.01 Service Pack 1, however we recommend installing Internet Explorer 4.01 Service Pack 2 (Not Internet Explorer 5.0 or later).

3. Install Microsoft Windows NT 4.0 Option Pack.
4. Install Microsoft Proxy server 2.0.
5. Install Microsoft Windows NT 4.0 Service Pack 4 or Service Pack 5 (Do not install Y2K updates as these are installed by MDAC 2.1 Service Pack 2.)
6. (Optional) Install Microsoft Internet Explorer 5.
7. Install MDAC 2.1.2.4202.3, also known as MDAC 2.1 Service Pack 2.
8. Install Microsoft Windows NT 4.0 Service Pack 6a or later.

   NOTE: Even if the latest service pack is installed in step 5, you must reinstall the latest pack at this point as the Windows NT Option Pack replaces certain DLLs.

9. Install Proxy 2.0 Service Pack 1.

3.2.1.3. Integration with ICAP proxy (ICAP mode)

Once OPTENET has been installed you must configure the caches or appliances so that they can use the OPTENET ICAP server as the filtering system (see section 3.5).

3.2.1.4. Without an additional proxy (Stand-Alone mode)

The element installed to capture the requests in the stand-alone version is the OPTENET proxy. The OPTENET proxy is a simple proxy distributed by OPTENET that is run when the operating system is started.
This allows you to use the OPTENET filter without additional products. The data captured by the OPTENET proxy is the same as the data mentioned for the Microsoft Web Proxy. The OPTENET proxy does not need a special plug in and it communicates directly with the OPTENET filter via remote procedure call (RPC).

You must keep in mind that the filter can only carry out the filtering if the HTTP requests are redirected via the proxy. Therefore, it is necessary to explicitly enter the proxy in the browsers' configurations.

Please check Appendix 4 for how to configure OPTENET proxy.

3.2.1.5. Specific information for Windows 98 and Windows Me

In Windows 98 and Me the system services concept is different, both OPTENET Server and OPTENET Proxy and OPTENET Reporter are installed as common processes and are automatically started when the operating system is started.

3.2.2. On Linux, Solaris and Aix systems

The distribution of OPTENET consists of the following files:

- optenet-5.27.XX-2.03.XX.tgz – The file containing the OPTENET Server and OPTENET Reporter software on Linux and Aix systems, and optenet-5.212.00-2.10.00.tar.Z on Solaris.
- install.sh - The installation script.
- OPTENETManual.pdf – User documentation.
- OptenetDCAgent.2.00.xx zip– File containing the software to install on your Windows server if you are using user authentication against an NT Domain.

install.sh is a shell script, so it can be opened and modified when required. During installation, install.sh creates a user to whom the OPTENET software will belong. By default, this user is called optenet, but you can edit install.sh to change the name. You can also change the root directory of the user, i.e. the OPTENET installation directory (/usr/local/optenet, by default). The user is created without a password but can be assigned one with the passwd command. The same thing happens if you also decide to install OPTENET Reporter. By default the user "reporter" is created, with its installation directory (/usr/local/reporter).
After creating the user, the installation script decompresses the optenet-5.27.tgz file in the installation directory and customises the OPTENET scripts.

During the installation process, the installer will ask if you want OPTENET to work as an ICAP server to be integrated with appliances that support this protocol, or to be integrated with Border Manager from Novell or with Cisco PIX Firewall or if it should be integrated with the SQUID version that is distributed with it. Likewise, if you have the license code corresponding to the product, the installer will you to register this code.

3.2.2.1. Installation of OPTENET as an ICAP server (ICAP mode)

The ICAP option should be selected when OPTENET is going to be installed on a network that already has caches or appliances (NetCache or BlueCoat machines, for example) that support the ICAP 1.0 protocol. In this case the OPTENET start up scripts will be created so that OPTENET starts its ICAP server whilst it waits to receive filtering requests from it. Once OPTENET has been installed, the caches or appliances should be configured so that they use the OPTENET ICAP server as a filtering system, (see section 3.5).

3.2.2.2. OPTENET installation with SQUID (SQUID mode)

The SQUID option installs a version of the modified SQUID proxy together with OPTENET so that it communicates with OPTENET via RPC (Remote Procedure Call) every time that it attends a request to connect to the Internet. In this case, the OPTENET start-up scripts are modified so that OPTENET and SQUID are started simultaneously. Although by default SQUID listens to requests at port 8080 you can change the port by

editing the squid/etc/squid.conf file in the installation directory and modifying the label http_port. The squid/etc/squid.conf file allows you to configure many aspects of SQUID's operation. We recommend that you read it thoroughly and that you adjust it to your requirements. Once OPTENET has been started you must configure your network browsers so that they use SQUID as a proxy and this way the filtering can be carried out.

With the default installation in SQUID mode, SQUID does not recognise users. To configure Squid with the user recognition option you must edit the squid/etc/squid.conf file, change the auth_param tag with the authentication you require, add an entry in the ACL (access control lists) and allow this entry in the access, For example, if you wan to used basic authentication using a flat text file of users and passwords you have to add the following lines to the configuration file:

```
auth_param basic program /usr/local/optenet/squid/libexec/ncsa_auth /usr/local/optenet/squid/etc/passwd
auth_param basic children 5
auth_param basic realm OPTENET Server
auth_param basic credentialsttl 2 hours

acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

From this moment, the first time each user wants to access the Internet via the proxy, he or she will be asked for identification (username - password) to be able to use the Internet. This username can be used later when forming rules with OPTENET. By default, no user is defined. We can create a user using the Perl script located in the tools/adduser.pl directory in the installation directory, in the following way:

perl adduser.pl usuario password fichero_password

for example:

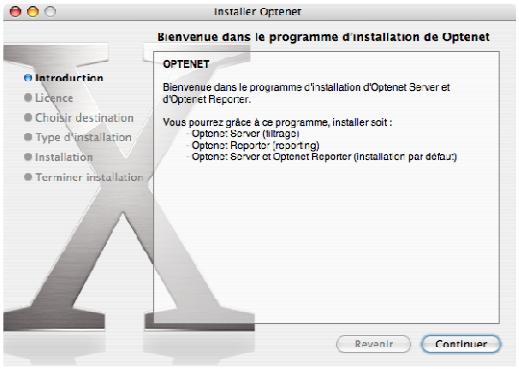
```
# perl adduser.pl luis clave_luis ../squid/etc/passwd
```

3.2.3. Under Mac OS X

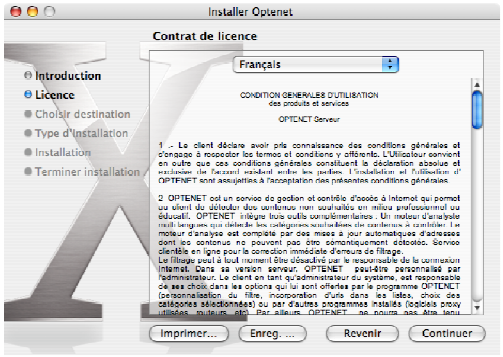
Under Mac OS X, the distribution of OPTENET involves the following files:

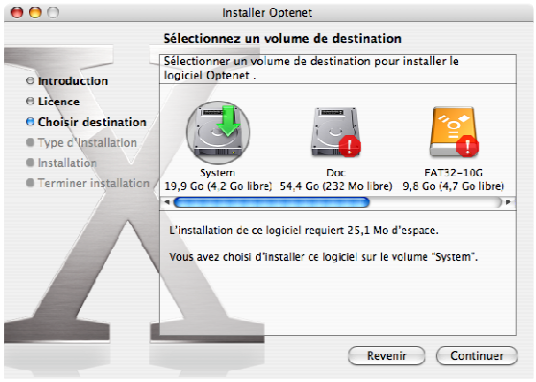
- optenet-5.21.dmg
- OPTENETManual.pdf – user's manual.
- OptenetDCAgent2.00.xx.zip – software file to be installed on your Windows server, if user authentication with an NT domain is employed.

In order to install OPTENET Server on your server, double click on optenet-5.21.dmg. A new volume will then appear in the Finder. Next, double click on Optenet.mpkg to launch the installation procedure. By default, the installation wizard starts up in the language of your operating system. If the language in question is not one of the three that are available, it will start up in English.
The installation software's welcome window will then be displayed. Click on Next to view the general conditions of use.

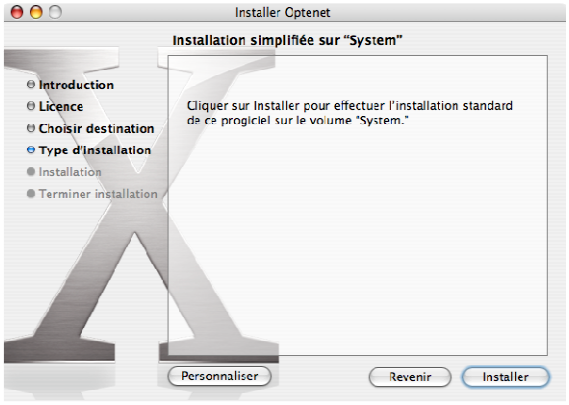


You may then print or make a note of the general conditions of use. When you click on Next, you will be asked to accept or reject these conditions.

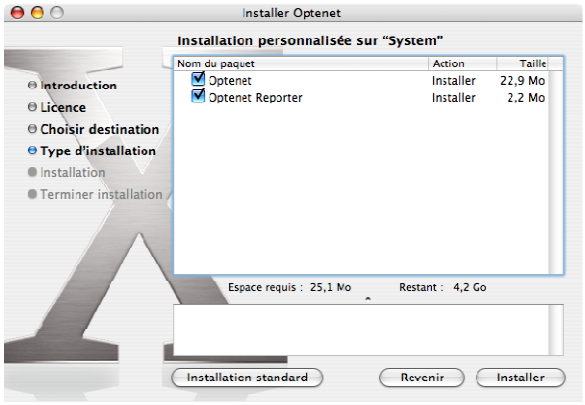


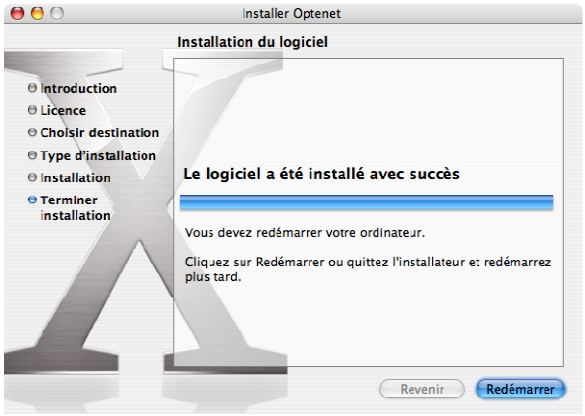


Next, you need to select the target volume. OPTENET must be installed on the volume corresponding to the operating system, which is indicated by a green arrow.



You will subsequently be able to launch the installation of OPTENET Server and OPTENET Reporter by clicking on the Install button. If you only want to install one of the components, click on the Customise button and select the component in question.





The software is installed. OPTENET and its Squid proxy are launched automatically when the system is started up.

3.2.4. System for files installed by OPTENET

OPTENET Server installs the following files and directories from its installation directory:

manager.html HTML page that redirects to the OPTENET Server WWW Administration.
optenet.html HTML page that redirects to the company OPTENET's WWW.

- **bin** directory: where the OPTENET Server DLLs and executable files are stored.
optenet.exe The OPTENET Server service executable file in linux.
Optenet_service.exe The OPTENET Server service executable for Windows NT, Windows 2000, Windows XP and Windows 2003.
Optenet_process.exe The OPTENET Server process executable for Windows 98 y Windows Me.
messages.dll *The DLL with the OPTENET Server events messages. Only in Windows*.
metabase.dll *DLL with auxiliary functions for the installation and un-installation of OPTENET Server. Only in Windows.*

- **etc** directory: with OPTENET Server configuration files.
***.conf** OPTENET Server configuration files. These files are not encrypted and should not be modified. The configuration you be exclusively carried out through the OPTENET configuration web pages.
- **files** directory**:** with the URL Databases and the OPTENET Server analysers.
***useryes.edu** Files with the URLs that belong to the user categories. They are simple text files that can be modified to add, modify or delete URLs manually.
***usernot.edu** Files with the URLs that do not belong to the user categories. They are plain text files that can be modified to add, modify or delete URLs manually. Together with the *useryes.edu files they make up the local URL Database. At first they do not exist but they will be created as URLs are added.
- list.crp Encrypted, compressed file with the set of general URL lists categorised. In the case that one of the *.edu files is corrupted it will be unpacked to recover the data. This file appears after the second day.
- **listxxxx.crp** Files with the update of the general URL database and the OPTENET Server analyser. It is a compressed file that only appears during the manual process to reload full lists as it is deleted once the update has been carried out.

-categoryuserex.edu File with the description of the categories added by the administrator.
- **logs** directory: Where, by default, the logs generated by OPTENET Server are saved.
updates.log File with the results of the automatic updates carried out by OPTENET Server.
-**requestYYYYMMDD.log** File with all the HTTP requests made through OPTENET Server in day DD of month MM of year YYYY.
- **cluster.log** File with the information referring to the cluster management.
- **actions.log** File that is saved by the actions log on the administration.

- **manager** directory: Contains the information required for the HTML pages that make up the OPTENET Server WWW Administration.
index.html Default page of the OPTENET Server WWW Administration. Redirects to the WWW Administration in Spanish. You can change the default language of the OPTENET Server WWW Administration by changing this file.

- **esp** directory: Contains the OPTENET Server WWW Administration pages in Spanish.
- **eng** directory: Contains the OPTENET Server WWW Administration pages in English.
- **fra** directory: Contains the OPTENET Server WWW Administration pages in en French.
- **deu** directory: Contains the OPTENET Server WWW Administration pages in German.
- **ita** directory: Contains the OPTENET Server WWW Administration pages in Italian.
- **por** directory: Contains the OPTENET Server WWW Administration pages in Portuguese.
- **eus** directory: Contains the OPTENET Server WWW Administration pages in Basque.

- **cgi-bin** directory: Contains the JavaScript code used by OPTENET Server WWW Administration.

- **listclusters** directory: saves the executable file for the cluster management.

- **stop** directory: where the local stop page is hosted. There should be as many folders as languages available.
- tools directory with OPTENET Server utilities.
- logrotate.bat Utility to rotate OPTENET Server logs. Only on Linux and Solaris systems.
- optenetcli (cli.conf) Application to modify the parameters of the filter administration from the commands line.
- backup.bat Utility to provide OPTENET Server back-up copies.
- restore.bat Utility to restore the back-up copies made using the backup.bat utility.
- OptenetSnmp (snmp.conf): Executable file of the OPTENET Server SNMP Agent. Only on Linux.
- stunnellauncher Executable file to administer the filter in a secure way, https. Only on Linux.
- adduser.pl Script that adds a user for the NCSA Authentication with Squid. Only with Squid proxy and Linux systems.
- addplugin.vbs Script that adds the OPTENET Server plug in to Microsoft ISA Server. Only in Windows for ISA Server or Proxy Server.
- delplugin.vbs Script that deletes the OPTENET Server plugin from Microsoft ISA Server. Only in Windows for ISA Server or Proxy Server.

Apart from the files that are installed from the installation directory, OPTENET Server installs the following:

- a file in the Microsoft ISA Server installation directory (by default C:\Program files\Microsoft ISA Server). This file is called **optenet.dll** and is the DLL that performs the tasks of a OPTENET Server data capturing ***plugin***.

3.3. Start-up and shut down

3.3.1. On Windows systems

3.3.1.1. Starting and stopping the filtering on Windows NT, XP, 2000 and 2003

The main part of OPTENET Server is its filtering service. This service can be administered from Windows Services like any other service: you can start it, stop it, establish its start type, etc.

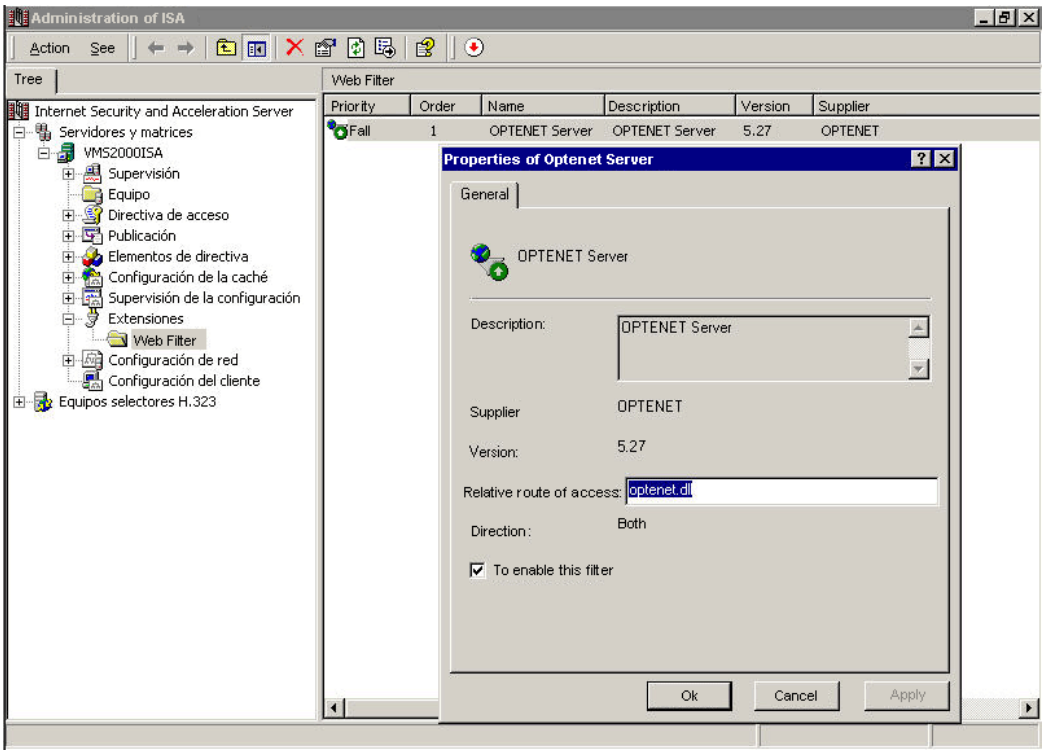
Starting the OPTENET Server service requires a certain amount of time (around 3 seconds) during which almost 100% of the server's CPU is used: the URL databases and the analysers in the memory are loaded, the automatic update process and OPTENET Server WWW Administration are started. If a problem occurs OPTENET Server writes a message in the server's Events viewer.

3.3.1.2. Starting and stopping the filter in Windows 98

In Windows 98 the system services concept is different, both parts, the OPTENET proxy and the OPTENET server, are installed as common processes. They are started when the operating system is started.

3.3.1.3. The plugin for Microsoft ISA Server

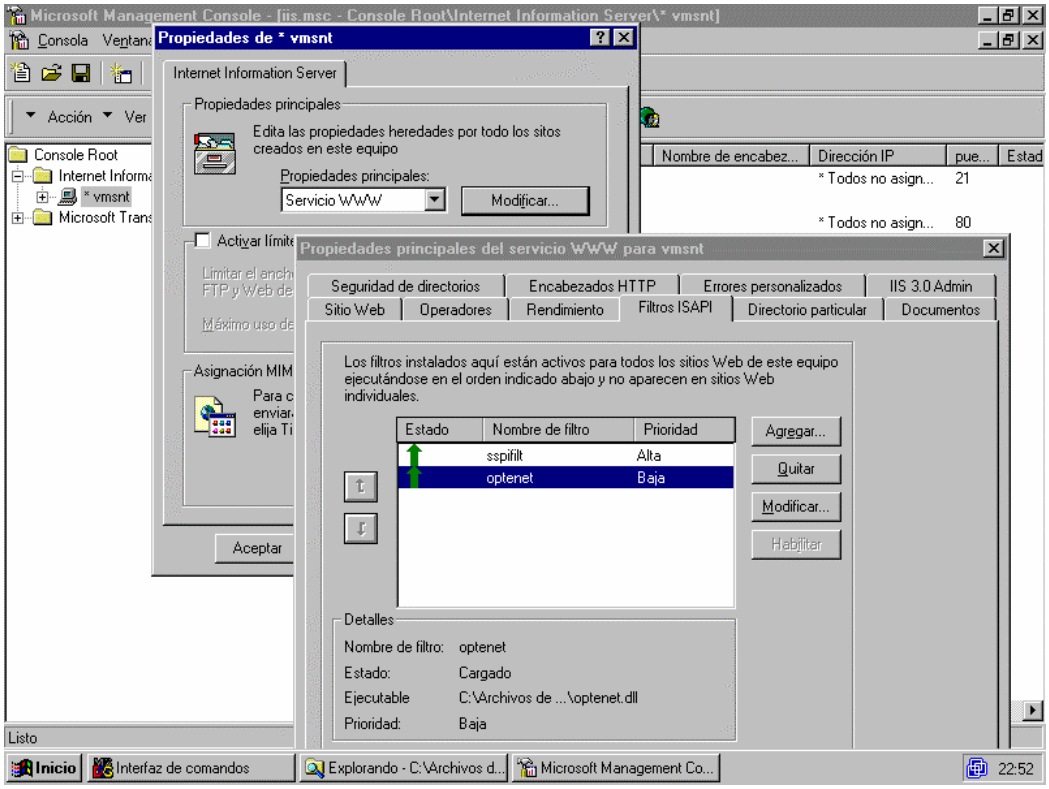
The other part of OPTENET Server, the data capturing plugin, is a Microsoft ISA Server Web Filter and it can be controlled from the ISA server Administration. Like any other Web Filter, it can be activated or deactivated as required (see the next figure). You can also start it or stop it via the Microsoft Web Proxy service (see Section 3.2.1.1).



The two parts of OPTENET Server are independent and they can be started or stopped separately, however, in order for the filtering to be produced both parts should be working correctly at the same time.

3.3.1.4. Microsoft Proxy Server Plugin

The other part of the OPTENET Server is the data capture plugin. This is an ISAPI filter installed on the same web server as the Proxy Server. This can be controlled from the Proxy Server Administration Console. Like any other ISAPI filter it can be activated or deactivated as needed. (see the following figure).



The two parts of OPTENET Server are independent and they can be started or stopped separately, however, in order for the filtering to be produced both parts should be working correctly at the same time.

3.3.1.5. OPTENET proxy

In the stand-alone version the OPTENET proxy is integrated and it processes the HTTP and HTTPS requests instead of Microsoft ISA Server. Its icon is visible on the toolbar. In the event that an additional proxy needs to be used in tandem its IP address and port should be entered in the proxy configuration window. Keep in mind that for normal use without an additional proxy it is not necessary to add any type of configuration in this section. Please see Appendix 4 for how to configure this proxy.

3.3.2. On Linux, Solaris and Aix systems

To start OPTENET enter the system as the newly created user and execute the filterinit script. This script admits the parameters start, stop and restart.
To start the filter, execute:

```
# ./filterinit start
```

To stop it, execute:

```
# ./filterinit stop
```

To restart the filter, execute:

```
# ./filterinit restart
```

If you have difficulties with the installation, please e-mail use at support@optenet.com for technical support.

3.3.3. Under Mac OS X

To start up OPTENET, access the system via the terminal utility. To do so, you will need to be working in administrator mode. Enter the following command:

```
# sudo su - optenet
```

Enter your password. This script accepts the start, stop and restart parameters.
Run the following command to start up the filter:

```
# ./filterinit start
```

Use the following command to stop it:

```
# ./filterinit stop
```

Additionally, it can be restarted by means of the following command:

```
# ./filterinit restart
```

If you experience problems during installation, technical support can be obtained by writing to info@optenet.com

3.4. Automatic starting and stopping with the system

3.4.1. On Windows systems

The default configuration after the installation is for the filter to be started and stopped automatically with the system. If you do not want it to start with the system go to the "System Administrator" System Tool and in the "Services" section change the "Start type" of the "OPTENET Server" service to 'Manual',

3.4.2. On Linux systems

By default OPTENET starts up and shuts down at the same time as the system. To set up OPTENET as a manually controlled service on the server you need to connect as the root user and follow these steps:

On Linux systems with the chkconfig (Red Hat) tool installed:

```
# cp /usr/local/optenet/optenet/tools/optenet /etc/rc.d/init.d
# chkconfig --add optenet
```

You can check that OPTENET has been installed as a service with the command:

```
#chkconfig –list
```

On Linux systems without chkconfig:

```
# cp /usr/local/optenet/optenet/tools/optenet /etc/init.d
# cp -s /etc/init.d/optenet /etc/rc.d/rc3.d/S99optenet
# cp -s /etc/init.d/optenet /etc/rc.d/rc3.d/K99optenet
```

3.4.3. On Solaris systems

By default OPTENET starts up and shuts down at the same time as the system. To set up OPTENET as a manually controlled service on the server you need to connect as the root user and follow these steps:

```
# cp /usr/local/optenet/tools/optenet /etc/init.d
# link /etc/init.d/optenet /etc/rc2.d/S99optenet
# link /etc/init.d/optenet /etc/rc2.d/K99optenet
```

3.4.4. On Aix Systems

By default OPTENET starts up and shuts down at the same time as the system. To set up OPTENET as a manually controlled service on the server you need to connect as the root user and follow these steps:

```
# cp /usr/local/optenet/tools/optenet /etc/rc.optenet
# mkitab "optenet:2:once:/etc/rc.optenet. start"
```

3.4.5. Under Mac OS X

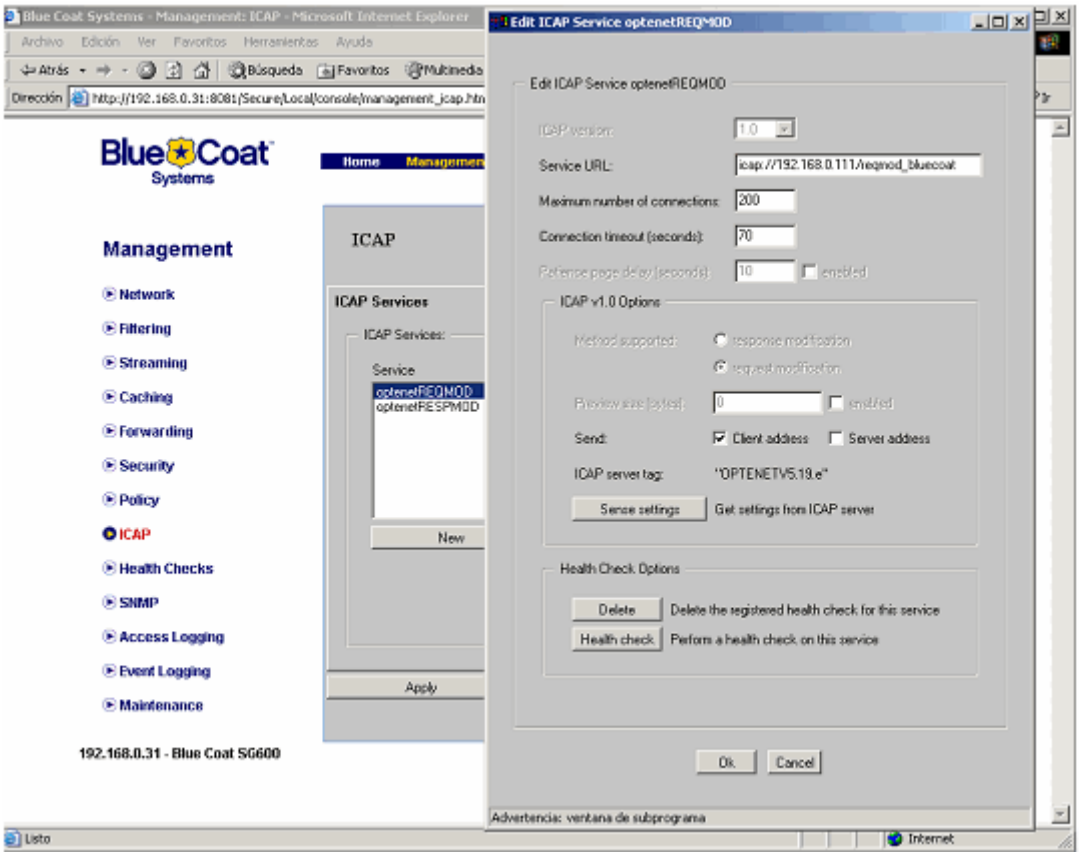
With the default configuration and following installation, OPTENET starts up and shuts down automatically when the system does so. Mac OS X runs OPTENET automatically thanks to the “Optenet” script, which is located in /Library/StartupItems/Optenet.

3.5. Configuration of a BlueCoat Appliance so that it uses OPTENET as a filtering system (ICAP)

In order for OPTENET to be able to communicate via the ICAP protocol with its BlueCoat Appliance it must have the Security Gateway 2.1.06 or later Operating System installed. Below we describe how a BlueCoat Appliance (before CacheFlow) should be configured so that it uses OPTENET as the filtering system. To do this you must follow these steps:

3.5.1. Creating a request modification service (REQMOD)

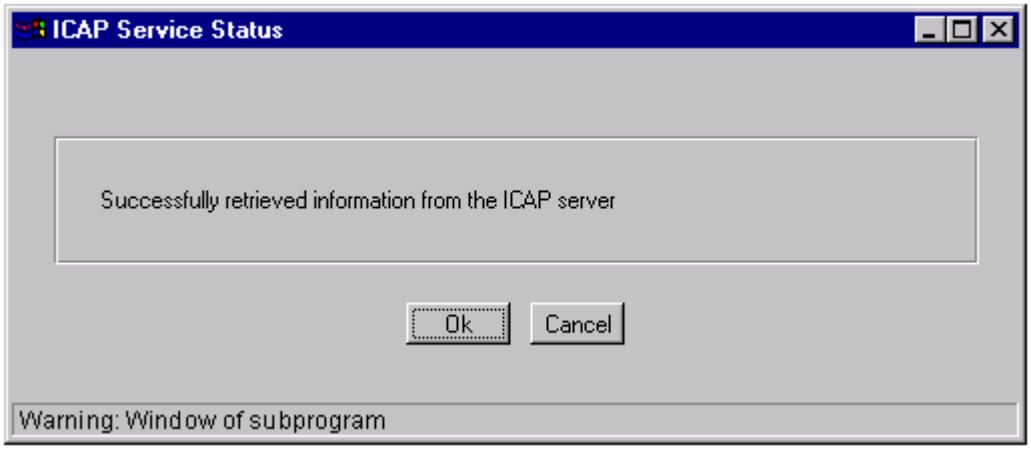
Connect to the BlueCoat administration and go to the ICAP option. In ICAP Services click on “New” and create one as shown in the figure:



In “ICAP version” you must assign version 1.0 of ICAP. In the “Service URL” sections you must specify the URL against which the ICAP requests will be sent, e.g.:

icap://192.168.0.111/reqmod_bluecoat

Note that the IP corresponds to the IP of the machine where OPTENET was installed and that /reqmod_bluecoat was used as the route. It is CRITICAL that this naming is used for the correct integration of the ICAP server OPTENET uses with BlueCoat. You should now select “request modification” as the method and use the button “Sense settings” to force BlueCoat to connect with OPTENET and therefore automatically obtain the rest of the configuration parameters from the ICAP server.



If for some reason the communication with the ICAP server fails, you can configure the rest of the fields manually. You must also select “Client address" (available from version

SG 2.1.07 onwards) to activate in the ICAP message the sending of the IP address of the client that made the request.

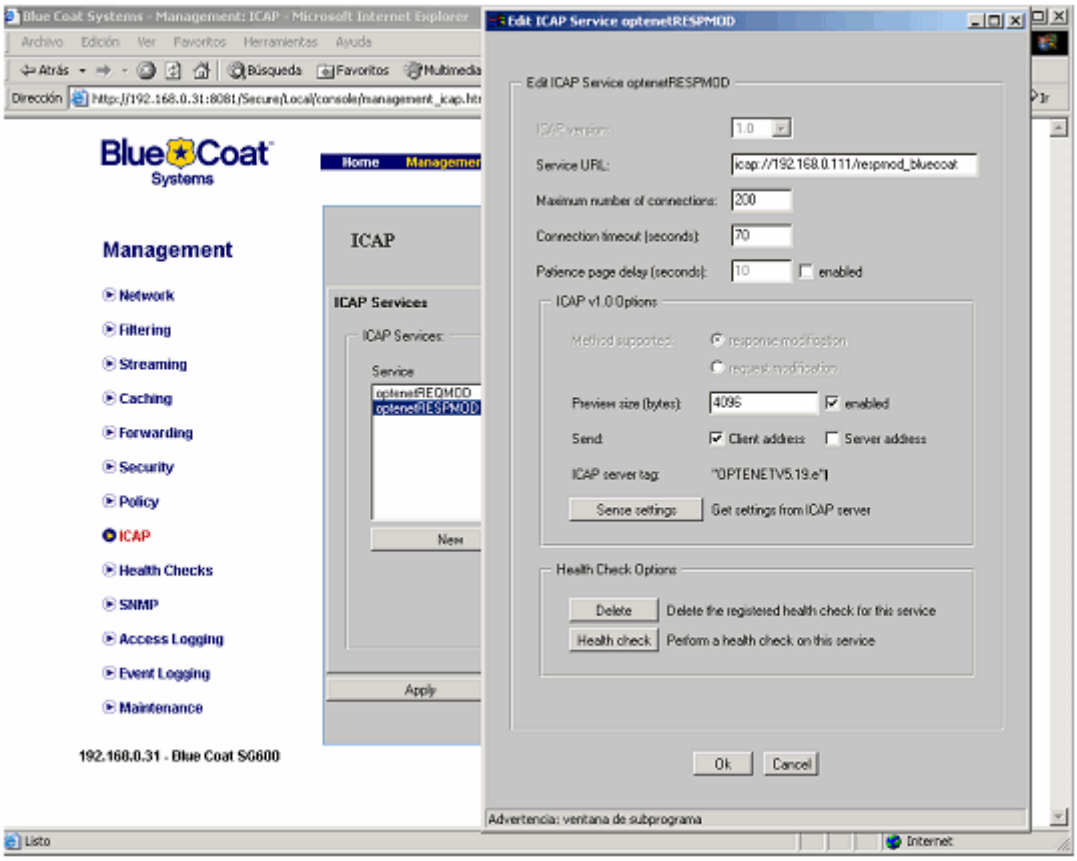
3.5.2. Creating a response modification service (RESPMOD)

Connect to the BlueCoat administration and go to the ICAP option. In ICAP Services click on “New” and create one as shown in the figure:

In “ICAP version” you must assign version 1.0 of ICAP. In the “Service URL” sections you must specify the URL against which the ICAP requests will be sent, e.g.:

icap://192.168.0.111/respmod_bluecoat

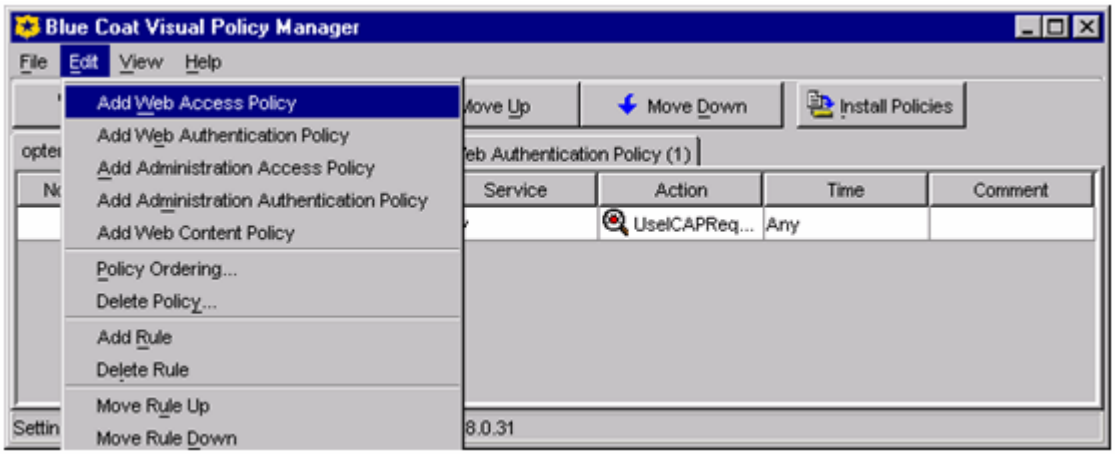
Note that the IP corresponds to the IP of the machine where OPTENET was installed and that /respmod_bluecoat was used as the route. It is CRITICAL that this naming is used for the correct integration of the ICAP server OPTENET uses with BlueCoat. You should now select “request modification” as the method and use the button “Sense settings” to force BlueCoat to connect with OPTENET and therefore automatically obtain the rest of the configuration parameters from the ICAP server. You must also select the “Client address" (available from version SG 2.1.07) to activate in the ICAP message the sending of the IP address of the client that made the request.



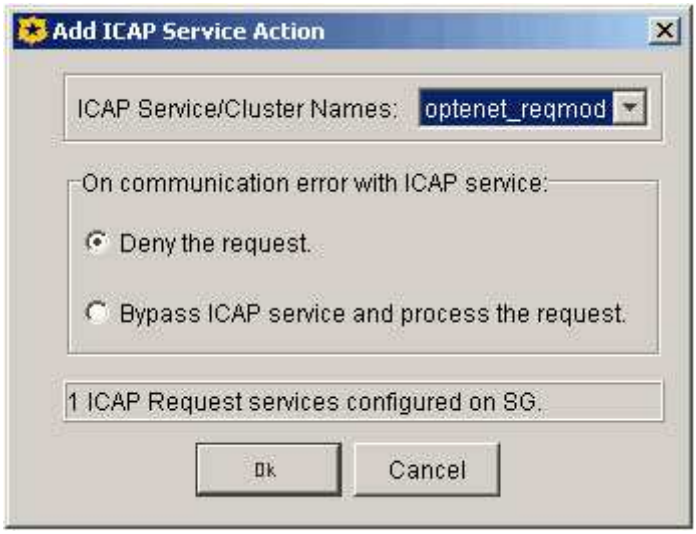
3.5.3. Establishing a web access policy

Once the ICAP services have been defined, we must indicate that all the requests are to be redirected against OPTENET. To do this, go to the Policy option, Visual Policy Manager and Start button to start the Visual Policy Manager.

Once it is started, select the following menu Edit -> Add Web Access Policy as indicated in the figure:



And configure the action of the new policy so that all the requests from all the clients use the ICAP service that we have called optenetreqmod. This way, we are informing BlueCoat that it should send the requests to OPTENET before carrying out all the web accesses made through it, so that they can be analysed and it can determine if they should be allowed or denied.

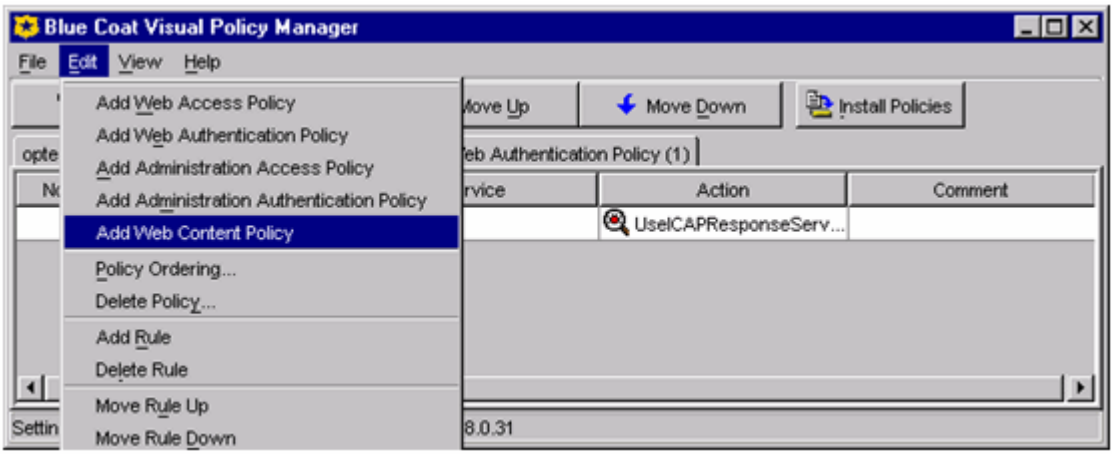


To save the changes in the Appliance click on “Install Policies” before closing the Visual Policy Manager.

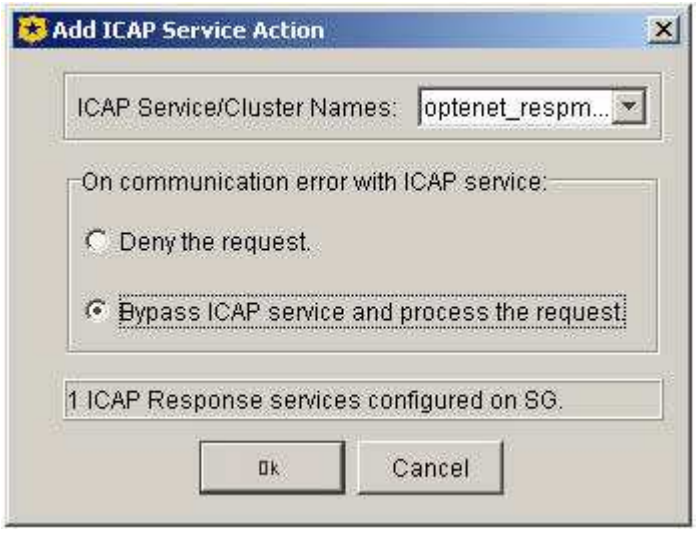
3.5.4. Establishing a web content policy

Contrary to most filtering systems, OPTENET analyses the content downloaded from the Internet enabling you to categorise pages by their content or to detect the real type of renamed files. For this purpose, BlueCoat must send OPTENET the content downloaded before returning it to the client that has requested it.

This is achieved by defining a web content policy. To do this, go to the Policy option, Visual Policy Manager and click on Start to start the Visual Policy Manager.
Once it has been started, select the menu Edit -> Add Web Content Policy as indicated in the figure:



And configure the action of the new policy so that the contents of all the requests from all the clients use the ICAP service that we have called optenetreqmod. This way, we are informing BlueCoat that before returning all the web contents downloaded through it to the clients, it should send them to OPTENET so that they can be analysed and it can determine if they should be allowed or denied.



To save the changes in the Appliance click on “Install Policies” before closing the Visual Policy Manager.

If you wish to activate user authentication you should start the Visual Policy Manager and create a Web authentication policy. Consult the BlueCoat documentation for more information.

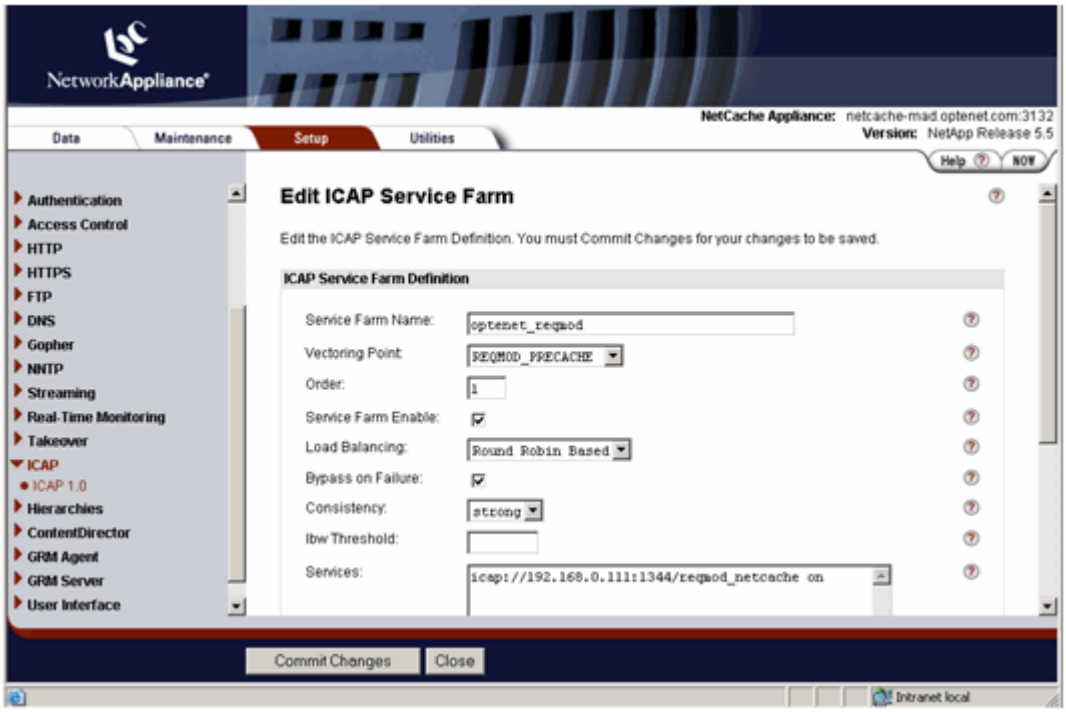
Once this last step has been completed your BlueCoat is now configured to use OPTENET as the filtering system.

3.6. Configuring NetCache to use OPTENET as the filtering system

Below we describe how to configure NetCache to use OPTENET as the filtering system. To do this you must follow these steps:

3.6.1. Creating a request modification service (REQMOD)

Connect to the NetCache administration and go to the option Setup→ ICAP → ICAP1.0. In ServiceFarm click on “New Service Farm” and create one as shown in the figure:



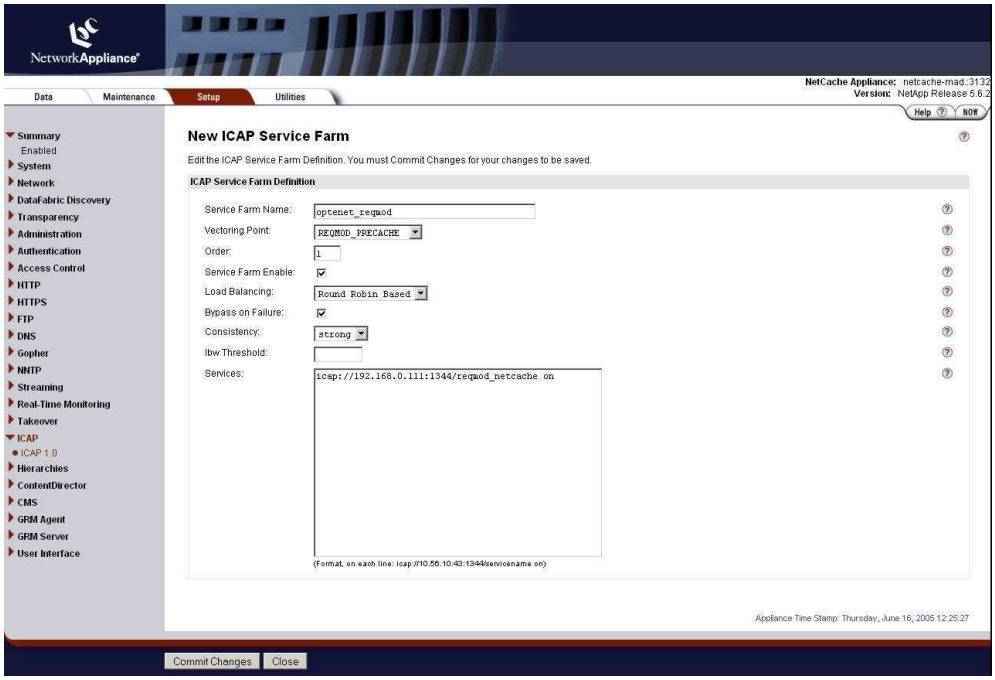
In “services” you must specify the URL to which the ICAP requests are sent, for example:

icap://192.168.0.111:1344/reqmod_netcache on

Note that the IP corresponds to the IP of the machine where OPTENET was installed and that /reqmod_netcache was used as the route. It is CRITICAL that this naming is used for the correct integration of the ICAP server OPTENET uses with NetCache.
Click on “Commit Changes” to save the changes.

3.6.2. Creating a response modification service (RESPMOD)

Create a new Service Farm a shown in the following figure:

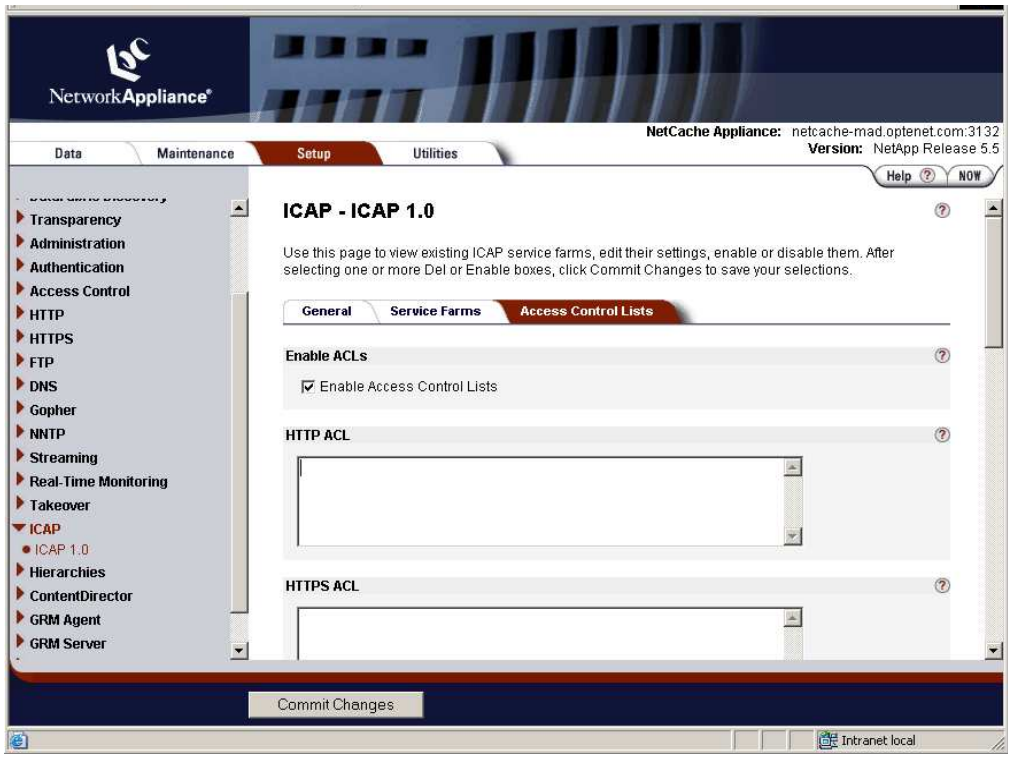


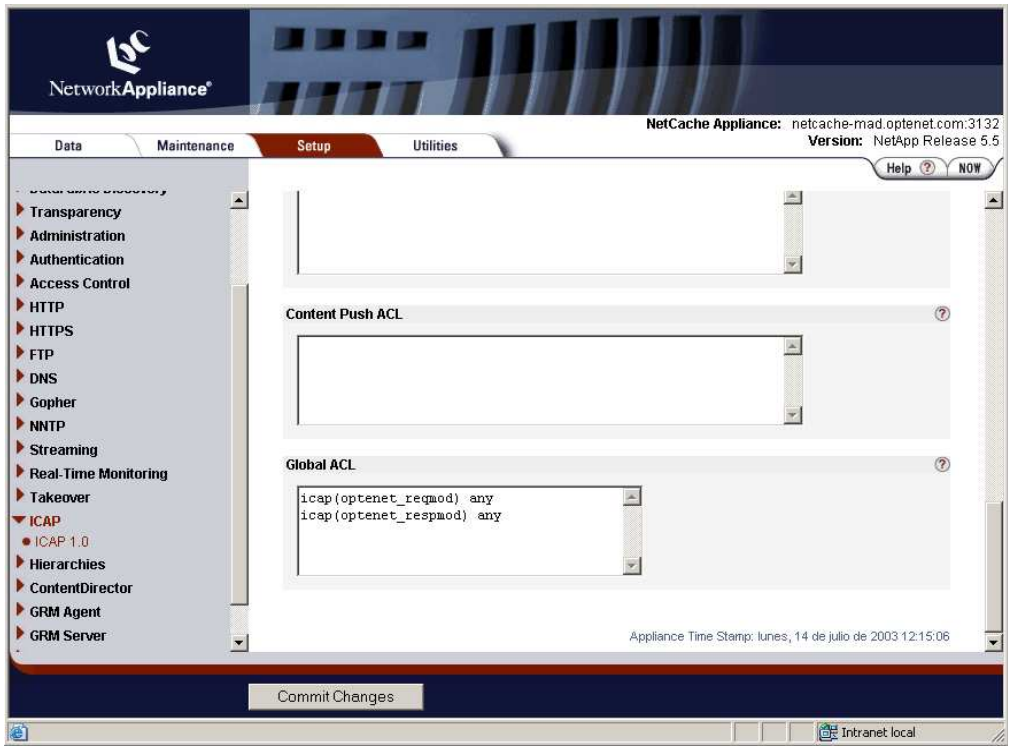
In the services box the ICAP request URL should be specified, for example:

icap://192.168.0.111:1344/respmod_netcache on

Note that the IP corresponds to the IP of the machine where OPTENET was installed and that /respmod_netcache was used as the route. It is CRITICAL that this naming is used for the correct integration of the ICAP server OPTENET uses with NetCache.
You have to create two Service Farms because OPTENET unlike most filtering systems analyses the content downloaded from the internet permitting the pages to be categorized according to the context or detect the true file type if this has been renamed. The first Service Farm means that when NetCache receives a request, before attending it, it sends the requested URL to OPTENET so that it can decide if access should be allowed. This decision is taken into account by checking the URL against the OPTENET database and analysing the actual URL.
The second Service Farm means that when NetCache retrieves a content from the Internet, before storing it in its cache, it sends the content to OPTENET. OPTENET will analyse it and it will decide if it should be allowed or blocked.

Once the Service Farms have been defined, you should indicate which requests the filter will be applied to. To do this, go to the Access Control List option and configure as shown in the figure:

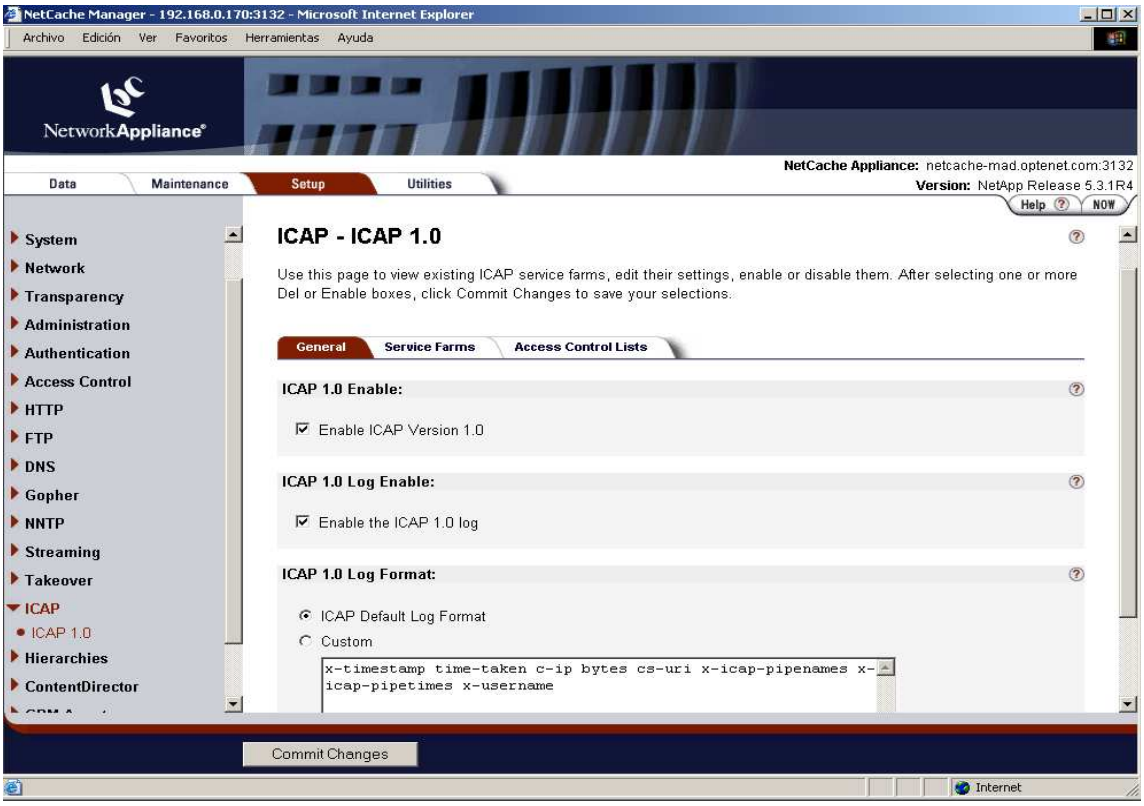




That is to say, by applying the filter to all requests, http, https and ftp requests.

Lastly you simply have to activate the ICAP service from the General tab as shown in figure.

If you want to activate user authentication you should consult your NetCache documentation.


NetCache Manager - 192.168.0.170:3132 - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
NetworkAppliance
NetCache Appliance: netcache-mad.optenet.com:3132
Version: NetApp Release 5.3.1R4
Data Maintenance Setup Utilities
Help NOW
System
Network
Transparency
Administration
Authentication
Access Control
HTTP
FTP
DNS
Gopher
NNTP
Streaming
Takeover
ICAP
ICAP 1.0
Hierarchies
ContentDirector
ICAP - ICAP 1.0
Use this page to view existing ICAP service farms, edit their settings, enable or disable them. After selecting one or more Del or Enable boxes, click Commit Changes to save your selections.
General Service Farms Access Control Lists
ICAP 1.0 Enable:
Enable ICAP Version 1.0
ICAP 1.0 Log Enable:
Enable the ICAP 1.0 log
ICAP 1.0 Log Format:
ICAP Default Log Format
Custom
x-timestamp time-taken c-ip bytes cs-uri x-icap-pipenames x-icap-pipetimes x-username
Commit Changes
Internet

4. BASIC CONCEPTS

Some basic concepts will be explained below, which are necessary in order to be able to properly administer OPTENET. These concepts will appear in the administration part.

4.1. User

Given that OPTENET communicates with a proxy (like Squid, ISA or OPTENET proxy), or with an appliance or cache that serves as a proxy (like BlueCoat or NetCache) the concept of a user is the same as the concept of a user for these proxies. This means that OPTENET recognises the users that are identified by the proxies. **Warning**, these users can be independent from the users of the operating systems of all the machines that access the Internet via the proxy.
However, OPTENET also allows User Authentication based on NT domains or LDAP servers (see section 5.4).

4.2. Group

Users can normally form part of one or various groups. Neither ISA, nor SQUID, nor any versions of BlueCoat prior to 3 pass on to OPTENET information regarding the groups to which the user who is making the request belongs. Only NetCache and BlueCoat after version 3 inclusive provide this information. This means that OPTENET, in order to be able to obtain this information, must communicate with some NT dominion or LDAP server. With regard to the configuration of this service, read Section 5.4 of this manual.

4.3. IP address

TCP/IP are the abbreviations for Transmission Control Protocol/Internet Protocol, the language that governs all communications between computers on the Internet. All computers connected to the Internet have a unique address assigned, with the following format:
aaa.bbb.ccc.ddd

As part of an OPTENET rule, it is going to be possible to include the IP addresses of all client computers who are going to access the Internet.

However, you must bear in mind that on occasions a linked proxy is placed before the filter and this may cause all the requests to be identified with this proxy's IP; consult your proxy's configuration if this effect occurs when not required.

4.4. URL

This is the abbreviation for Uniform Resource Locator. It is the address of a site or source, normally a directory or a file, on the World Wide Web and the convention that browsers use in order to find files and other distant resources. A URL can identify a file, for example:

http://www.optenet.com/eng/index.htm

or a site:

http://www.optenet.com

With OPTENET, we can allow or block access to specific pages by indicating the URL, or allow or block access to entire sites or a part of them by indicating the URL followed by an asterisk. For example:

http://www.example.com/*

OPTENET works internally with URLs without a protocol (http, https, …). If we introduce a URL within a certain category, all the protocols for this URL will automatically belong to this category.
For example, if we introduce http://www.example.com within the pornography category, the following URLs will be categorized within pornography:
http://www.example.com
https://www.example.com
ftp://www.example.com

4.5. Category

A category is a set that groups together the files from the World Wide Web.
These sets may be created using URL lists and content analysers and URLs.

Five types of categories are established:
- Content categories: they classify the World Wide Web in contents (for example pornography, sports, press, etc.) that may be allowed or rejected as established in the filtering rules.
- White category: if a file belongs to a white category its contents categories will not be taken into account; it will be treated as if it did not belong to any content category.
- Black category: if a file belongs to a black category it will be treated as if it belonged to each and every one of the contents categories.
- Searchers category: the files belonging to a searcher category will not take the multilingual contents analyser into account to establish the content categories.
- Remailers category: these are files that readdress or transform other files. If a file belongs to a remailer category, the other file which is being readdressed or transformed will be worked on directly.

A category may have more than one type. In turn, a file may belong to more than one category.

Each category uses two URL lists for its definition: Yes and Not. The Yes list contains all

the addresses that we consider belong to a specific category and the Not list contains the addresses we consider do NOT belong to this category.

At the end of this manual there is an annex that describes the categories provided by OPTENET.

4.6. Rule

This is the basic concept on which OPTENET operation is based. The rules define the filtering level that all of our Internet accesses are going to have. With a rule, we can define:

- The categories on which a rule acts.
- The users affected by a rule.
- The user groups affected by a rule.
- The IP addresses of the stations affected by a rule.
- The types of files on which a rule can act.
- The times during which a rule must be applied.
- URLs to which a rule must be applied, irrespective of the category and type of file, which means that as long as the remaining characteristics are fulfilled (date and time and user, group or IP), the rule will act.
- URLs that will never fulfill the rule. In this manner, we can define exceptions to the action of each rule.

5. ADMINISTRATION

Once OPTENET server is installed, it is necessary to set up a minimum configuration. OPTENET Server incorporates a web server for its configuration and administration. This web server is installed at TCP port 10237 and allows OPTENET Server to be administered and configured using an internet browser.

If you have installed OPTENET Server on Windows you can go to the WWW Administration element in the OPTENET Server Programs Group (See Section 3.2.1) and the WWW Administration will open in the default browser you have configured on your system.

You can also access remotely from any computer connected to the network by accessing http://server:10237, where server will be the server with OPTENET Server.
If the equipment where OPTENET Server has been installed is a host.domain, it can access the Internet server at the following URL: http://host.domain:10237. In order to be able to access the Internet server, it is first necessary to have started OPTENET.

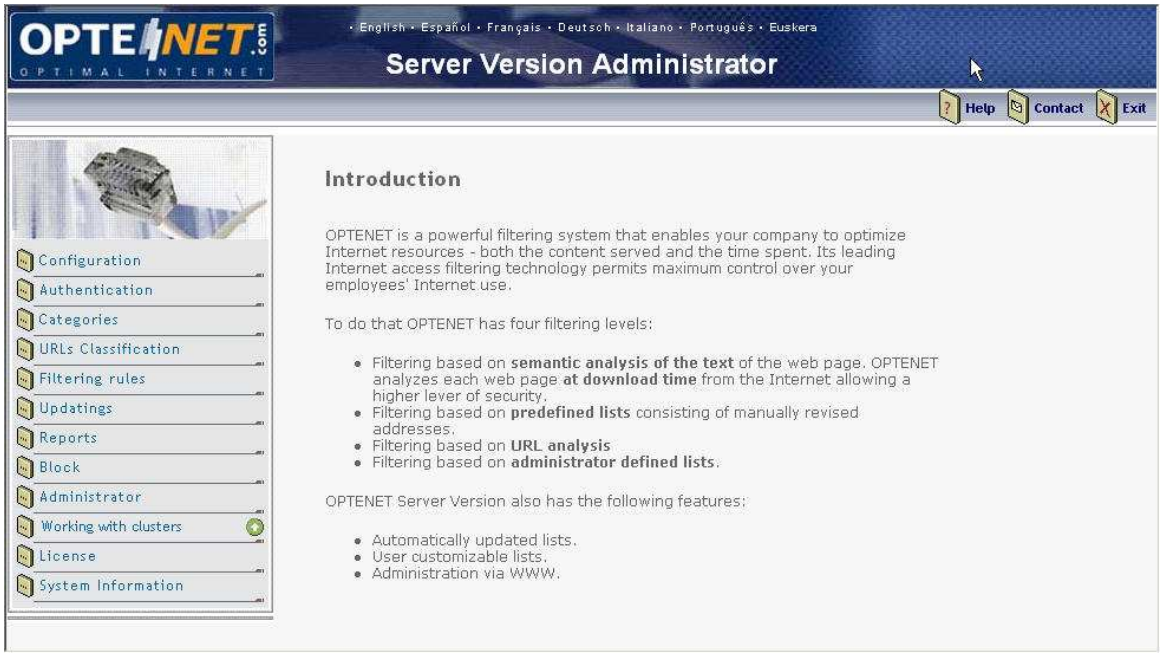
In order to ensure configuration and administration privacy, the Internet server requires the user to be authenticated, and it will therefore request the user name and password in a window like the one shown in Figure . By default, the user name is **optenet** and the password is **12345678**. These values can be changed from the Internet Administration server. It is recommended to change them as soon as OPTENET Server is installed.

Your browser might show a blank page when you introduce your user name and password. For correct access to the administration you must add the URL where OPTENET is installaed to your browser's trusted sites. For example, if OPTENET is installed on http://192.168.0.240 and it is using Internet Explorer 6.0, you must access the menu Tools -> Internet Options -> Security -> Trusted Sites and add here the URL http://192.168.0.240.

5.1. Introduction

It is the default window that appears when you enter the administration, once the user has been correctly authenticated.

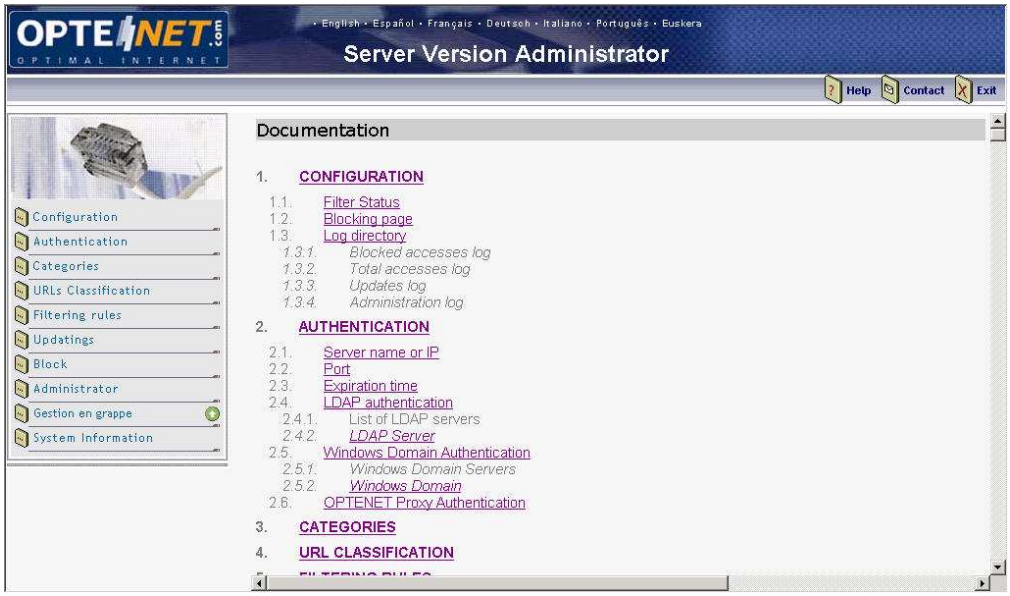
It gives a brief introduction about OPTENET. If you would like the administration web in another language you simply have to click on the flag of the desired language (under the OPTENET logo) and the administration will automatically appear in the chosen language. As an example, in Figure the introduction window is shown in French.


OPTENET.com
OPTIMAL INTERNET
· English · Español · Français · Deutsch · Italiano · Português · Euskera
Server Version Administrator
Help
Contact
Exit
Configuration
Authentication
Categories
URLs Classification
Filtering rules
Updatings
Reports
Block
Administrator
Working with clusters
License
System Information
Introduction
OPTENET is a powerful filtering system that enables your company to optimize Internet resources - both the content served and the time spent. Its leading Internet access filtering technology permits maximum control over your employees' Internet use.
To do that OPTENET has four filtering levels:
Filtering based on semantic analysis of the text of the web page. OPTENET analyzes each web page at download time from the Internet allowing a higher lever of security.
Filtering based on predefined lists consisting of manually revised addresses.
Filtering based on URL analysis
Filtering based on administrator defined lists.
OPTENET Server Version also has the following features:
Automatically updated lists.
User customizable lists.
Administration via WWW.

OPTENET.com
OPTIMAL INTERNET
· English · Español · Français · Deutsch · Italiano · Português · Euskera
Administrateur Version Serveur
Aide
Contactez-nous
Sortir
Configuration
Authentification
Catégories
Classification d'URLs
Règles de filtrage
Mises à jour
Rapports
Bloquer
Administrateur
Gestion en cluster
Licence
Information du système
Introduction
OPTENET est un système de filtrage qui permet d'optimiser les ressources d'Internet de l'entreprise ainsi que le temps employé. Sa technologie leader en sélection et en filtrage d'accès à Internet va permettre de contrôler au maximum l'utilisation d'Internet de tous les ordinateurs connectés au réseau.
Il existe quatre niveaux de filtrage :
Filtrage en fonction de l'analyse sémantique du texte qui apparaît sur la page web. OPTENET analyse chaque page lors de son téléchargement d'Internet, en permettant un meilleur niveau de sécurité en fonction des listes.
Filtrage d'après des listes prédéfinies avec les adresses classées manuellement.
Filtrage d'après l'analyse des URL.
Filtrage d'après des listes prédéfinies par l'utilisateur.
En outre, OPTENET Version Serveur présente les caractéristiques suivantes :
Mise à jour automatique des listes.
Personnalisation des listes prédéfinies.
Configuration par WWW.

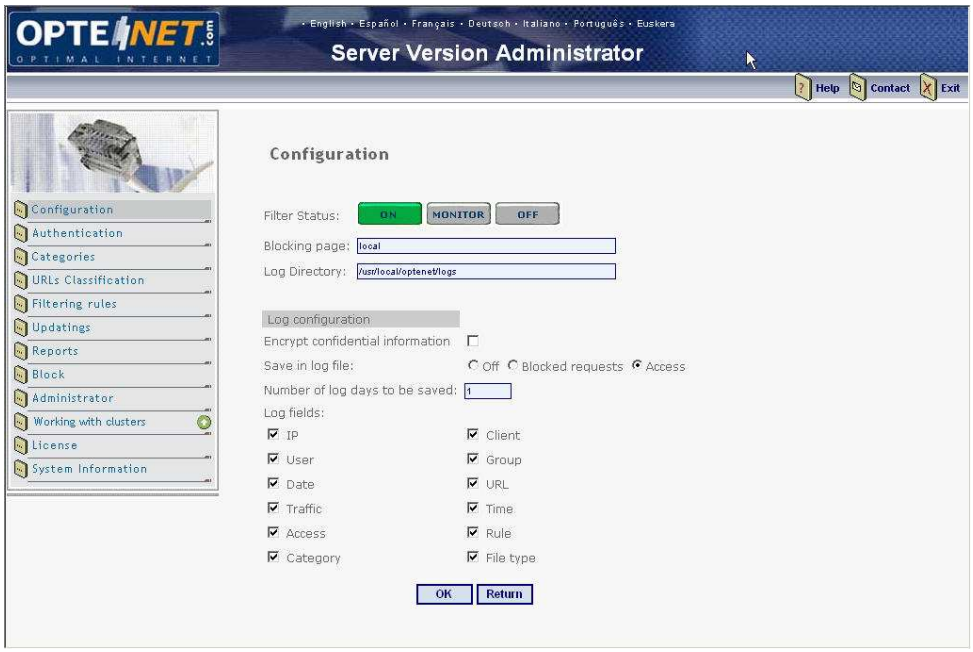
5.2. Documentation

Shows the documentation in HTML format.



5.3. Configuration

Within this option, you can configure aspects such as the filter status, establish the blocking page or establish the directory where the logs are generated. We will now look at each one of these options.



5.3.1. Filter Status

The filter currently allows three states:

- ON: active state, the filter processes all the requests applying the actions established in the filtering rules. This is the default configured state that allows the filter to block access.
- MONITOR: a state where all the requests are processed, simulating the application of the filtering rules and allowing writing on the logs, but **without filtering.** Useful for installations that want to carry out an analysis phase on their browser before applying the filter.
- OFF: inactive state, the filter immediately responds to all the requests received, letting them through, without blocking any access.

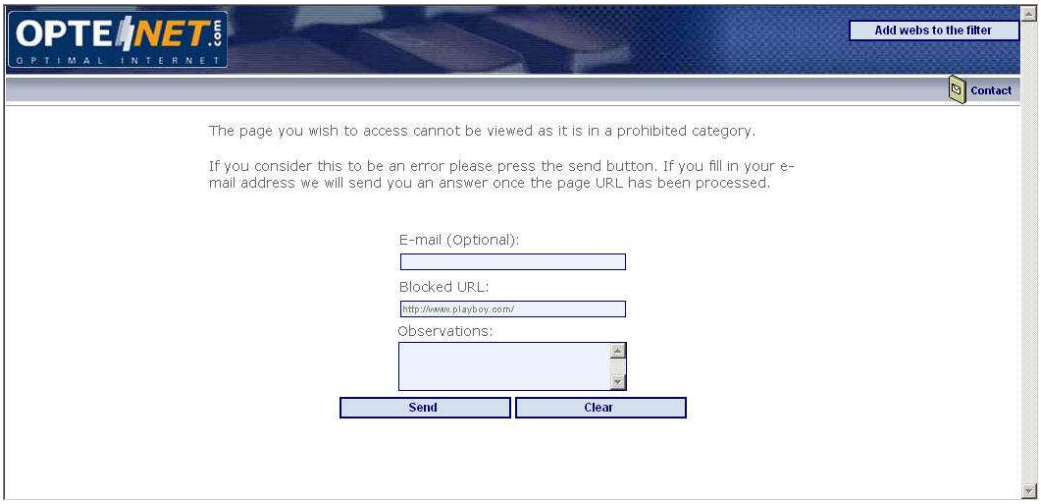
OFF should not be confused with stopping the filter. Even though we may select the OFF status, OPTENET Server continues to run, but it stops monitoring accesses to the Internet. In order to stop the filter, you must be connected as user optenet in a telnet session against the Linux, Solaris or Aix server and you must enter ./filterinit stop or stopping the Windows service or process.

5.3.2. Blocking page

OPTENET Server allows you to personalise the messages that are displayed to the users when a page they have attempted to access is blocked.. By default in the field appears the key word “local”. This way, the it shows the local blocking page located in the installation directory (see section 3.2.3 System of files installed by OPTENET). In order for the local blocking age to be shown correctly, it is necessary for the filter to be able to obtain the local ip of the server where it is being executed. Ensure that there is an entry of the type “ip server name” in the “hosts” configuration file. It is also necessary that all the equipment which is used to navigate has access to the blocking page. In the event that the “local” configuration cannot see the blocking page, try making the blocking page: http://ip_del_servidor_optenet:10237/cgi-bin/stop. Supposing that OPTENET is executed in the ip 192.168.0.235 the blocking page would be:

http://192.168.0.235:10237/cgi-bin/stop

Next Figure shows the default OPTENET Server blocking page. It is usual to create your own personalised web page and locate it in the intranet of your organisation and to establish it as the OPTENET Server blocking page.


OPTENET.com
OPTIMAL INTERNET
Add webs to the filter
Contact
The page you wish to access cannot be viewed as it is in a prohibited category.
If you consider this to be an error please press the send button. If you fill in your e-mail address we will send you an answer once the page URL has been processed.
E-mail (Optional):
Blocked URL:
http://www.playboy.com/
Observations:
Send
Clear

The HTML response pages can be generated dynamically through a CGI or an ASP page. In this case, we must indicate the complete URL of the CGI/ASP as the blocking page.

If the response pages are generated dynamically, the information that OPTENET Server sends to the blocking page can be included. The response CGI/ASP receives the following variables in the query string (GET method):

- **URL** → indicates the URL that has been blocked.
- **DATETIME** → date and time when the request is made.
- **RULE** → rule that has blocked that URL.
- **CAT** → category to which the blocked URL belongs.
- **FILE** → type of file of the blocked URL.

If you have also activated the sending of the username and IP as the stop page parameter, then you will receive two further parameters:

- **USER → the name of the user making the request.**
- **IP → the IP for the machine from which the request is made.**

The sending of these parameters is disabled by default for security reasons. If you wish to activate it, you need to set the value as **TRUE** in the Windows register code:
HKEY LOCAL MACHINE\SOFTWARE\OPTENET\OPTENET Server\SendIpUser
If you have installed OPTENET Server on a Linux, Solaris or Aix system, then you should modify the **/usr/local/optenet/RunOPTENET** script adding as the optenet_server parameter **-send_ip_user TRUE**. On both platforms, you then need to restart the filter for the change to take effect.

This information can be very useful. We can use it to send an e-mail to the administrator or in order to receive statistics.

5.3.3. Log directory

In this section you can configure the directory where OPTENET will save the logs. OPTENET Server keeps the following types of log.

5.3.4. Log configuration

5.3.4.1. Encryption of sensitive information

Enabling this option will force OPTENET to writ the IP, username and groups to which the user making each request belongs to the logs in encrypted form. The default is for this option to be disabled.

5.3.4.2. Save to log

From here the user can select which information OPTENET will save on the log files (requestYYYYMMDD.log). The following values can be selected:

- **Nothing**, indicates that the filter will not save any of the requests received for analysis to the log, i.e., the logs will not be saved.
- **Only blocks**, indicating that the filter will only save those requests which have been blocked to the logs.
- **Accesses**, indicating that the filter will save all requests sent for analysis, i.e. both the ones blocked and the ones allowed to pass.

5.3.4.3. Number of days' information to be saved

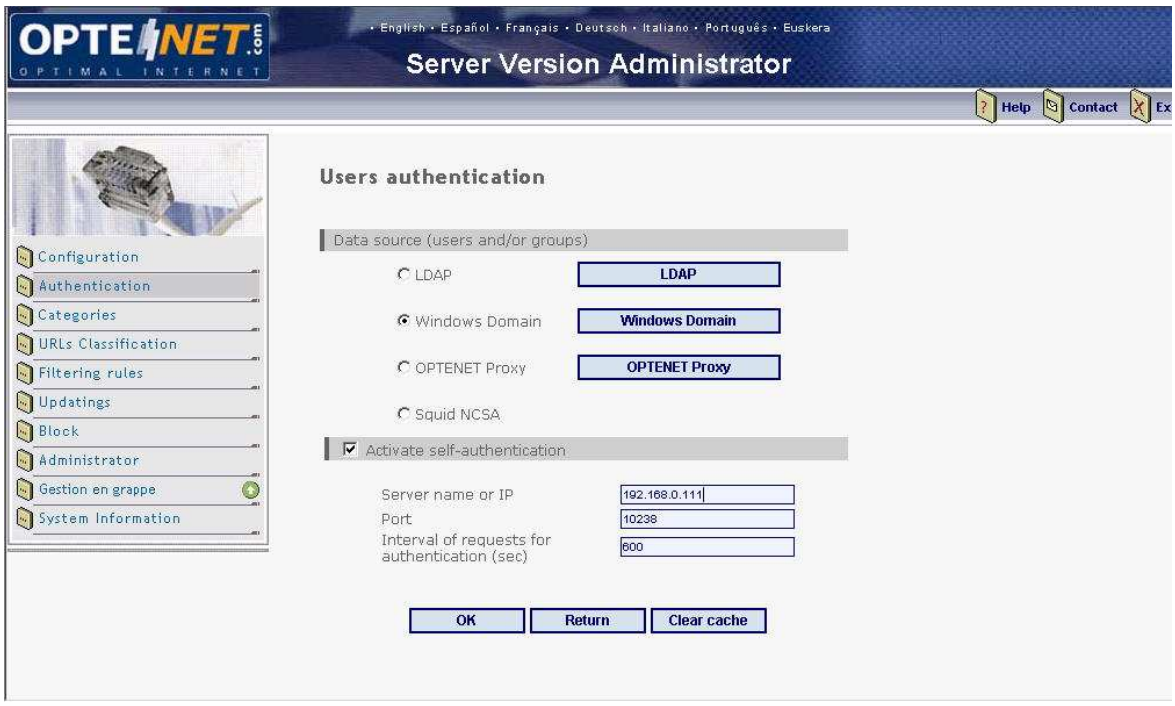
Here the user can configure the number of complete days' log information that he/she wishes the filter to save. By default, the value is 1, which indicates that the filter will always keep the complete logs from the previous day, and those for the current day. When the date changes, the filter will delete all logs prior to the period of days specified.
Contrary to other, earlier versions of OPTENET Server, where the report module was integrated with the filter and where the logs were accumulated in the filter log directory, in this version the filter does not accumulate logs. OPTENET Reporter is the option which, once installed and configured, requests the configured filters for the logs they have and accumulates the data received from each filter in its own directory of logs. The fact that OPTENET Reporter stops working temporarily and OPTENET Server continues to operate does not mean that the logs generated during this timeframe are lost and reports about them cannot be obtained. The next time that OPTENET Reporter is opened it will start to ask OPTENET SERVER for the logs generated since the last time it received any. As a result, if these logs have not yet been deleted by the file, they can be recovered by the Reporter. One day's information for saving should be sufficient for the Reporter and the filter to synchronise their logs without any problem.

5.3.4.4. Log fields

From here the user can freely select the fields he/she wishes to include in the OPTENET Server logs. Bear in mind that disabling any of the fields mean that reports cannot be obtained later about this information using OPTENET Reporter; e.g. if the user field is disabled, it will not be possible later to obtain reports sorted or grouped by username.

5.4. Authentication

If you wish to establish filtration rules by users or by groups of users, the proxy or appliance needs to be configured to perform user authentication or for OPTENET to carry out this authentication directly. Otherwise you will only be able to set the filtration rules by the IP's of the equipment accessing Internet.



5.4.1. Data origin (Users and/or groups)

Should you wish to establish filtration rules by users and/or groups OPTENET can supply the listing of users and groups fro the section users/groups within each filter rule. For OPTENET to be able to display this information, you need to, in the section "Authentication" -> "data origin" select which source of data will be used by OPTENET to obtain the users and groups. Additionally, as was mentioned in section 4.2, most proxies or caches (in fact, none of them except for NetCache and BlueCoat as of version 3 inclusive) do not send to the filter the groups to which the user who is making the request belongs, Therefore, OPTENET needs to discover this information. Selecting the type of data source and appropriately configuring each possible source, OPTENET will be able to list the users, the groups and ask each user's group.

There follows a description of the data origins with which OPTENET is able to work.

5.4.1.1. LDAP

Select the LDAP option if your organisation manages user and group accounts with LDAP servers. Examples of these servers are Windows Active Directory, Lotus Domain and iPlanet. After selecting the LDAP option and clicking on the accept button in the "User Authentication" window, you should click on the LDAP button to define how many LDAP servers are necessary.

Clicking on the LDAP button, you will access the configuration window for LDAP servers.

5.4.1.1.1. List of LDAP servers

In this section, LDAP servers are configured with which OPTENET Server will communicate to obtain the user and group listings and consult a user's group. OPTENET allows more than one LDAP server to be defined.
When consulting a user's groups, OPTENET will always consult the first server defined in the list and then consult the following if the former does not respond or if that user is not defined in the former. The order in which these servers are established is therefore fundamental. When listing all users or groups, OPTENET will consult all servers and show the total users and groups obtained.
From this option, a new LDAP server may be added or an existing one modified or erased and also their order established.

5.4.1.1.2. LDAP server

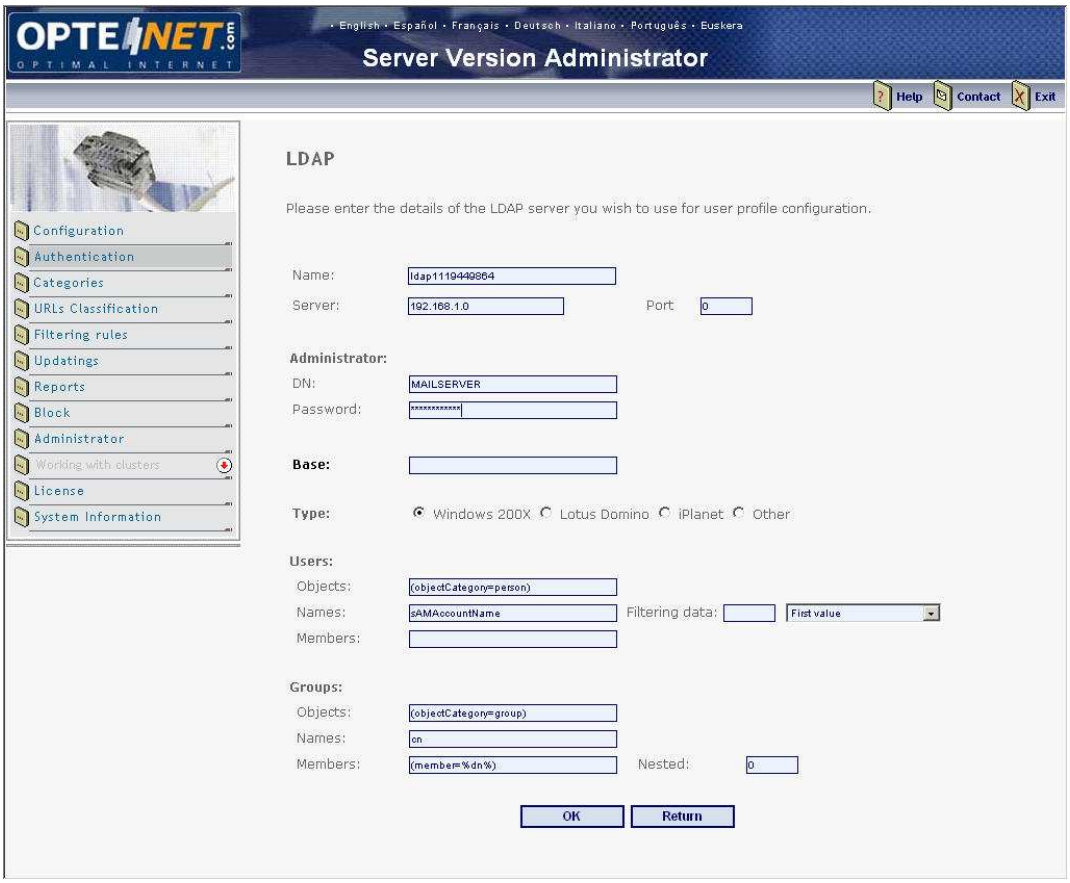
In this section, the selected LDAP server is configured. On adding a new server a new entry is created with a random name and with the standard LDAP port 389. The following data must be configured for each LDAP server:

- Name: The name with which This LDAP server is to be identified within the list. This name is purely symbolic but must be unique within the LDAP server list that it defines.
- Server: name or IP address of the LDAP server. We recommend inserting, whenever possible the IP address so that the LDAP enquiries are faster and do not have to resolve the name of each of them.
- Port: Port where the LDAP server is listened.

- Administrator: DN and access code of the LDAP server. If the LDAP server allows anonymous listening, they may be left empty.
- Base: base for user and group searches.
- Type: type of LDAP server.

The type of LDAP server is used to indicate to the filter the way in which the users and groups are to be obtained and the relation between each. To obtain that information the filter needs the following data:

- User objects: LDAP filter to search for objects with the user information, e.g. (objectClass=inetOrgPerson), (objectClass=rvUser) etc.
- Names of LDAP user attributes that will be used as a user name, e.g. shortname etc.
- Filtering criterion: When working with ICAP and a user identifier other than "**Distinguished name**" has been configured on LDAP, the option "consult user alias (LDAP)" must be activated and a maximum time set for the cache, as described later on in this manual. In this case, OPTENET will carry out a consultation in order to obtain the user identifier/s other than "**Distinguished name**". For OPTENET to know which of the identifiers described in the consultation it must use, this box exists so that a search pattern (for example "U*") can be used. In this respect, OPTENET shall only consider those fields that begin with U. Finally, in order to resolve possible cases with more than one match, a scroll-down exists which enables us to select "first value" or "last value".
- User members: condition that is applied to user objects to obtain the groups to which it belongs, e.g. (memberOf=cn=%cn%), (ou=%ou%) etc. Note that it can be indicated between % the object attributes that must meet the condition for the user to be considered a member of that group.
- Group objects: LDAP filter to obtain the objects with the group information, e.g. (objectClass=groupOfUniqueNames), (objectClass=rvGroup) etc.
- Group names: LDAP attribute that is used as a name for the groups, e.g. cn, ou etc.
- Group members: condition that is applied to group objects to obtain the users belonging to them, e.g. (uniqueMember=%dn%), (memberUid=%uid%) etc. Note that it may be indicated between % the attribute of the user objects that must meet the condition for the group to include that user as a member of it.
- Nested groups: maximum level of group nesting. A value of -1 is possible, in which case all the groups corresponding to a user will be searched for until there are no more nests. If the value is 0, nested groups will not be searched for. This must be used carefully, as more LDAP queries are performed per level, which can have a negative effect on performance.



There follows an example of an LDAP server configuration. In this example, the users consist of objects of inetOrgPerson type and their name is extracted from the uid attribute. The groups comprise objects of the type groupOfUniqueNames and their name is extracted from the cn attribute. To be aware of the groups to which users belong, only group objects are consulted (the section Members of Users is empty) and as a condition it is established that the attribute uniqueMember includes the user's uid in the format given. Nested groups will not be searched for.

5.4.1.2. Windows domains

Select the Windows Domain options if they manage user and group accounts in your organisation with Windows Domain, both NT and Windows 200 or 2003 installed in mixed mode. As a prerequisite, OPTENET DCAgent 2.xx must have been previously installed in a Windows server of your network that has access to the controllers of the domain that it is wished to consult. This software is responsible for consulting the domain controllers to extract users, groups and groups of each user. In turn, OPTENET server communicates with OPTENET DCAgent to obtain this information.

* This software can be downloaded from the OPTENET web. We also recommend that you consult your manual before installation.

5.4.1.2.1. **Windows Domain servers**

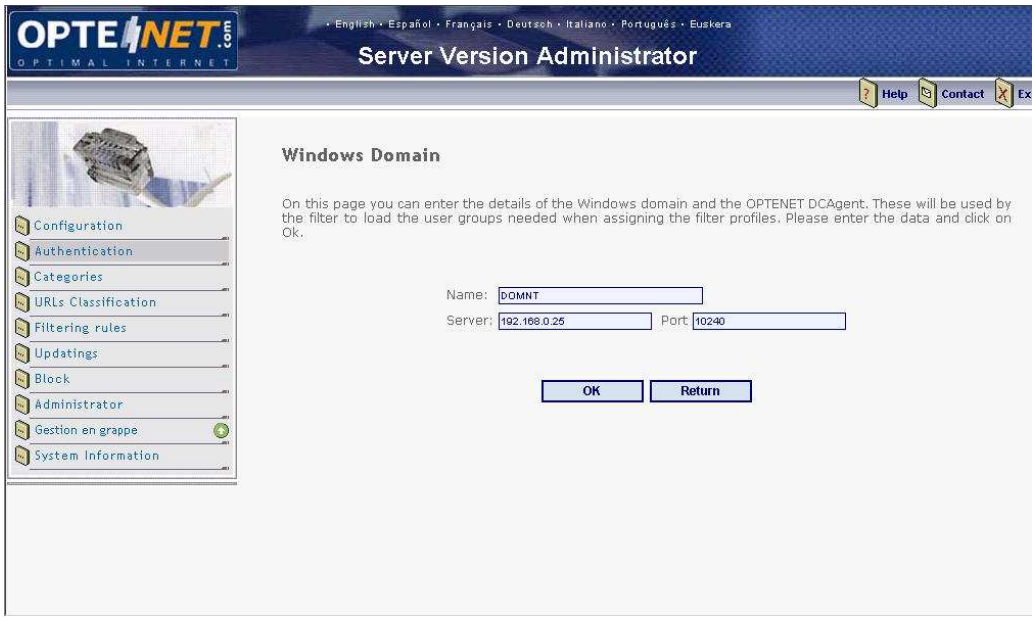
In this section, windows machines are configured is which OPTENET DCAgent 2.xx has been installed, with which OPTENET Server will communicate to obtain the user and groups listing and to consult the user groups. OPTENET allows more than one DCAgent to be defined.
When consulting a user's groups, OPTENET always consults the first server defined in the list and then consults the following if the former does not respond or if the user is not defined in the former. The order in which these servers are established is therefore fundamental. When listing all the users or groups, OPTENET will consult all the servers and show the total of users and groups obtained.

From this option, a new OPTENET DCAgent may be added, modified or an existing one erased and also their order may be set.

5.4.1.2.2. Windows domain

In this section the data of OPTENET DCAgent selected are configured. Adding a new server creates a new entry with a random name and with the standard listening port of DCAgent 10240. For each DCAgent server, the following data must be configured:

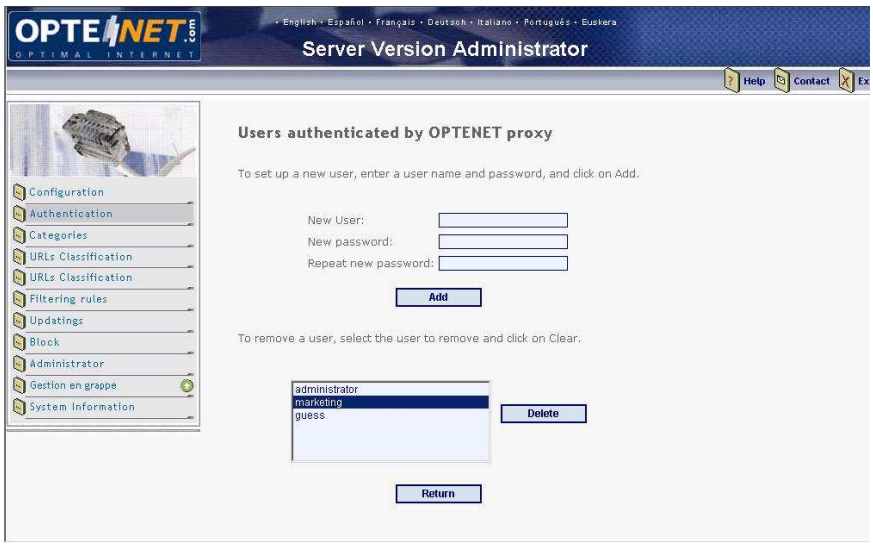
- Name: Name with which this server is to be identified within the list. This name is purely symbolic but it must be unique within the list of servers that it defines.
- Server: name or IP address where it is installed and executing the DCAgent CA. We recommend inserting, whenever possible, the IP address so that enquiries are faster and that the name does not have to be resolved in each of them.
- Port: Port where the DCAgent listens.



5.4.1.3. OPTENET Proxy

Select the OPTENET proxy option if OPTENET server has been installed in a Windows system and the OPTENET proxy has been selected in the installation. In this way, OPTENET will show, in the section “Filtration rules” -> “users”, the users that OPTENET proxy is able to authenticate. OPTENET proxy does not work with user groups and it is therefore not possible to establish rules by user group if your organisation is navigating through OPTENET proxy.

Clicking on the OPTENET Proxy button you will access the screen shown in figure, from where the users together with their access codes that OPTENET proxy is able to identify are added or eliminated. When introducing the first user together password, OPTENET proxy will begin to request authentication of each that navigates through it. When the last user is eliminated OPTENET Proxy will stop requesting user authentication.



5.4.1.4. Squid NCSA

Select the Squid NCSA option if OPTENET server has been installed in a UNIX environment (Solaris, Aix, FreeBSD o Linux), if the RPC option has been selected that installs squid together with OPTENET and also if Squid has been configured to request NCSA basic authentication. In this way, it will be able to make OPTENET show in the section “Filtration rules” -> “users”, the list of users that Squid is able to authenticate. Actually OPTENET carries out a search of the tag "auth_param basic program" of the configuration file of Squid (squid.conf) to obtain the user file, run it and, in this way, extract the user list. NCSA authentication of Squid does not work with groups of users and it is therefore not possible to set rules by group of users if your organisation is navigating through Squid in which NCSA authentication is configured.

5.4.2. Activating your own authentication

If your proxy or appliance is not configured to carry out user authentication, all users will be able to have internet access without identifying themselves introducing a user name and a password). This means that OPTENET does not receive the information of what user makes each request, not being able to apply filtration rules based on users or groups and only being able to establish different policies by the IP’s of users accessing Internet.
To be able to set filtration policies by user or group of users, we have two options:

- A) Configuring you proxy or appliance so that it performs user authentication (recommended option) or
- B) Configuring OPTENET so that it identifies the users who are navigating.

In the case of option A) in which it is the proxy or cache which is authenticating users, this proxy sends to OPTENET with each WEB request, the user who has requested it. OPTENET in this case must obtain the groups of this user for which it uses the origin of the data that have been configured (LDAP or Windows domains. We must remember that OPTENET proxy or Squid NCSA cannot establish filtration rules by groups).

Option B) consists of OPTENET identifying the users who are navigating. To activate it, the tick of the box “Activate your own authentication” should be marked in the user authentication window. This option can be useful for organisations in which the proxy/cache does not perform user authentication or where this cache does not send which user is making each request to the filter. In this way of working, OPTENET carries out an association between the IP’s that it receives with each request and those users navigating from these IP’s and it is therefore strictly necessary for those requests identified by their IP of origin to reach OPTENET and not by the IP of an intermediate gateway or router. There follows a description of the identification process performed by OPTENET:

1. A user begins an Internet session, carries out the web requests to the proxy and this passes them to OPTENET for it to decide whether to pass or block them.
2. OPTENET extracts the IP address of the request and checks it against its internal table that contains IP and user pairs.
3. As this IP is new, OPTENET does not yet know which user is behind this request. To find out, it has two methods:
   3.1 If the **“LDAP”** data origin is being selected, OPTENET redirects this request against its authentication server, requesting, at the same time, that the user who is navigating introduces a user and password and it will compare the data with the LDAP servers defined. To carry out these checks, the filter may query the “username” field as defined in the LDAP server or access the LDAP directory directly with the credentials supplied. Likewise, and only in the case where the “LDAP” is selected as the data origin, it is then possible to authenticate the user with the data contained in

the client certificate, using secure SSL communication. To do so, the LDAP database field to be queried has to be indicated for the certificate's content. If this last option is enabled and the data checked is erroneous, then a username and password are requested. Once checked, the relation between that IP and user is established so that all requests originating from that same IP will be considered as of that user during the "request interval of the authentication request", which may be defined in the same window.

3.2 If "**Windows Domain"** is being selected as data origin, OPTENET performs a request to the configured DCAgents requesting what user entered the session against the Windows domains from that IP. In this way, OPTENET is able to identify the user without it being necessary for the introduction of a name or password. This mode is also called **"Transparent authentication"** and, as may be imagined it is necessary for the user to have begun a session previously against a Windows Domain. Once this information is received from the DCAgent, OPTENET saves the relation between that IP and that user so that all requests originating from that IP will be considered from that same user during the "request interval of the authentication request", which may be defined in the same window.

3.3 If "**OPTENET Proxy**" is being selected as the data origin, the "activate own authentication" option will be ineffective and disabled. OPTENET extracts the user passing the request from the request that arrives from the proxy and there is no way of obtaining groups as the proxy does not send them. For OPTENET Proxy to request user authentication, one or more users will have to have been created in the "OPTENET Proxy" section.
3.4 If "**Squid NCSA**" is selected as the data origin, the "activate own authentication" option will be ineffective and disabled. OPTENET extracts the user passing the request from the request that arrives from the Squid and there is no way of obtaining groups as the proxy does not send them. For the Squid to request user authentication, it will have to have been properly configured. See the example in the section "Installing OPTENET with SQUID" in this manual.

4. Once the interval of "authentication request" has passed, sep 3 is repeated to check whether it is the same user who continues to navigate or whether it is a different user.

Summarising this point, OPTENET can perform user authentication as long as it receives the IP making the request and that the users begin the session against a Windows domain or have an LDAP server that can validate the users with their passwords.

It is not advisable for both the proxy/cache and OPTENET to perform authentication, as, in this case, OPTENET discards the user information which the proxy/cache sends it and tries to establish its own authentication.

5.4.3. Server name or IP

The IP or server name in which OPTENET is installed must be entered in this box. If this server has more than one network interface, the interface of the network that is accessible from the entire Intranet must be entered. In the event that this box is left blank, OPTENET obtains the IP address consulting the server directly. In the event that there are several OPTENET network interfaces, the first that is configured to coincide with the first shown for the command (ifconfig or ipconfig) is chosen.

This box is only valid if the user authentication has been activated. In order for OPTENET to be able to authenticate the LDAP users, the server where OPTENET is running must be accessible from all workstations of the Intranet (either directly or via the proxy), specifically the port where the authentication requests will be redirected. In this option, you can write in the IP of the machine that is “visible” from the entire Intranet or the name of the machine that is “visible” from the entire Intranet. Keep in mind that it is possible that you may have to add the machine’s name to your DNS server in order to resolve the authentication requests. If this field is left empty, OPTENET will use the one assigned to the machine by Windows.

5.4.4. Port

The OPTENET authentication server listens at this port. After changing the value of the port, you must restart OPTENET for the change to come into effect. The default value is 10238. This box is only valid if user authentication has been activated.

5.4.5. Interval of authentication request

It is the time indicated in seconds during which OPTENET considers valid the associations which it establishes between IP’s and users After this time in seconds has elapsed OPTENET will try to resolve the user as is indicated in the third point of the authentication process explained previously.

This time indicates the seconds during which OPTENET considers the association of a user with its groups to be valid. When this time elapses, when it receives the next navigation request from that user, OPTENET will again consult the groups of that user.

5.4.6. Carrying out a search for the DN associated to the username

So as to be authenticated, users have to provide a username and password that verify their identity with that held in the LDAP user database. This option serves to define the type of checks made for this username and password by OPTENET.

If this option is enabled, OPTENET carries out a search in the LDAP database to recover the DN from the record associated to the username entered. Once the DN has been recovered, OPTENET attempts to validate this DN alongside the password provided by the user.

If this option is disabled, OPTENET does not carry out a search in the database for the DN, instead it creates the DN directly from the username entered by the client. To do so, it concatenates the “username” field configured in the LDAP server with the value entered by the user and with the LDAP server base. Then, it attempts to validate the DN created with the password provided by the user, as above.

The main difference is that in the first case there is a guarantee that the DN used is correct, which allows for flexible configuration for any LDAP database. However, this option takes up more resolution time, as it requires prior consultation of the database. Whereas the second option does not guarantee correct searches and is only valid for rigid LDAP structures, in which all the DN are made up of the username and LDAP base.

Thus, this option is enabled by default.

5.4.7. Using client certificates

As we have mentioned above, OPTENET can obtain authentication credentials from client certificate data. To do so, this option has to be enabled.

On doing so, OPTENET's own authentication server becomes a secure server, which has to be accessed using an https protocol, rather than an http protocol. From this moment on, data transmission between OPTENET and the user is secure, using the SSL protocol.

Taking advantage of the possibility offered by SSL communications to send client certificates, OPTENET requests a digital certificate from users containing their credentials. Once received, OPTENET can validate the identity of this user using the information contained in the certificate, without the user having to enter their username and password.

5.4.8. LDAP field to verify the client certificate

To check that the digital certificate provided by a user coincides with the contents defined as data origin in the LDAP database, OPTENET has to consult the LDAP database.

To do so, OPTENET obtains the client certificate's digital fingerprint and compares it to the data in the LDAP field defined in this section. If the query is rejected, whether because the configured field does not exist or because there is no user associated to this digital certificate information, OPTENET offers the user the chance to authenticate themselves by entering a username and password.

5.4.9. Activation of user alias consultation (LDAP)

When working with ICAP or ISA Server, by activating this option OPTENET can work with an LDAP user identifier other than "**Distinguished name**".
Whatever the user identifier that has been configured on LDAP, in the request OPTENET receives the "**Distinguished name**" from the Appliance or ISA as the user identifier. In order solve the problem, OPTENET must carry out a consultation in order to obtain the user identifier configured on LDAP which corresponds to the "**Distinguished name**" received.
By default this option is deactivated. Once the option has been activated, the user-alias cache must be configured (following section of the manual) and the filtering criterion field must be established for each LDAP server that has been defined in the OPTENET administration.

5.4.10. Life period of the user-alias association

In order to avoid saturating LDAP servers by making a consultation for every ICAP request, OPTENET maintains an internal cache that associates a "**Distinguished name**" with the user identifier configured on LDAP. In this respect, the LDAP consultation is only made the first time. On subsequent occasions OPTENET uses the value stored in the cache. This cache has a maximum life period, after which the entries expire, which is when the LDAP consultation must be made again.
In this box the maximum life period must be entered in seconds.

5.5. Categories

OPTENET Server allows you to create and manage your own categories. In order to do so, you need only indicate the name and the types of category that you wish to create or erase, and the category will shortly be available throughout the filter.

The possible types are:

- content: content category.

  This type of category shall be treated in the same way as those categories that are included in the filter by default, which is to say the categories created by OPTENET. Once the category has been created, we can add URLs to same in the section “Classification of URLs” and subsequently use this category from filtering rules section.

- white: white category.

  In white categories, URLs can be included that will never be filtered for belonging to some category. There may be cases in which a URL belongs to more than one category; for example, a page from the finanical press will belong to the “press” category and the “economy” category, which means that it could be blocked in accordance with different filtering configurations. By including the URL in the “white” category, this URL will not be filtered at all. White categories are useful in enabling us to guarantee that the URLs included are not classified by any other category. Once the category has been created, we can add URL's to same in the section “Classification of URLs”.

- black: black category.

  Black categories exist for introducing URLs that we would like to be classified as belonging to all existing content categories. Once the category has been created, we can add URL's to same in the section “Classification of URLs”.

- search: searchers category.

  OPTENET will supply this category with the list of searchers. In addition, URLs can be included that will be treated like searchers. The difference with regard to the URLs included in this type of category will be that, when OPTENET Server analyzes them, it will use URL analysis instead of semantic analysis. This enhances effectiveness when it comes to authorizing or rejecting contents searched for by the user. Once the category has been created, we can add URL's to same in the section “Classification of URLs”.

- redirect: remailers category.

  OPTENET will supply this category with the list of remailers, anonymizers, etc. In addition, URLs can be included in order to facilitate closer examination of the typical functions of remailers. The special characteristic of this type of category is that when OPTENET Server analyzes the URLs included on the list, it also carries out a special search of the URL in an attempt to extract all the URLs contained in same, subsequently searching the categories of these inserted URLs. Once the category has been created, we can add URL's to same in the section “Classification of URLs”.

Bear in mind that you cannot add a category with a name that already existed before or erase a category that has not been added beforehand. At the same time, the pre-

established categories in the filter and those added by the administrator may not total more than 128 categories in all.

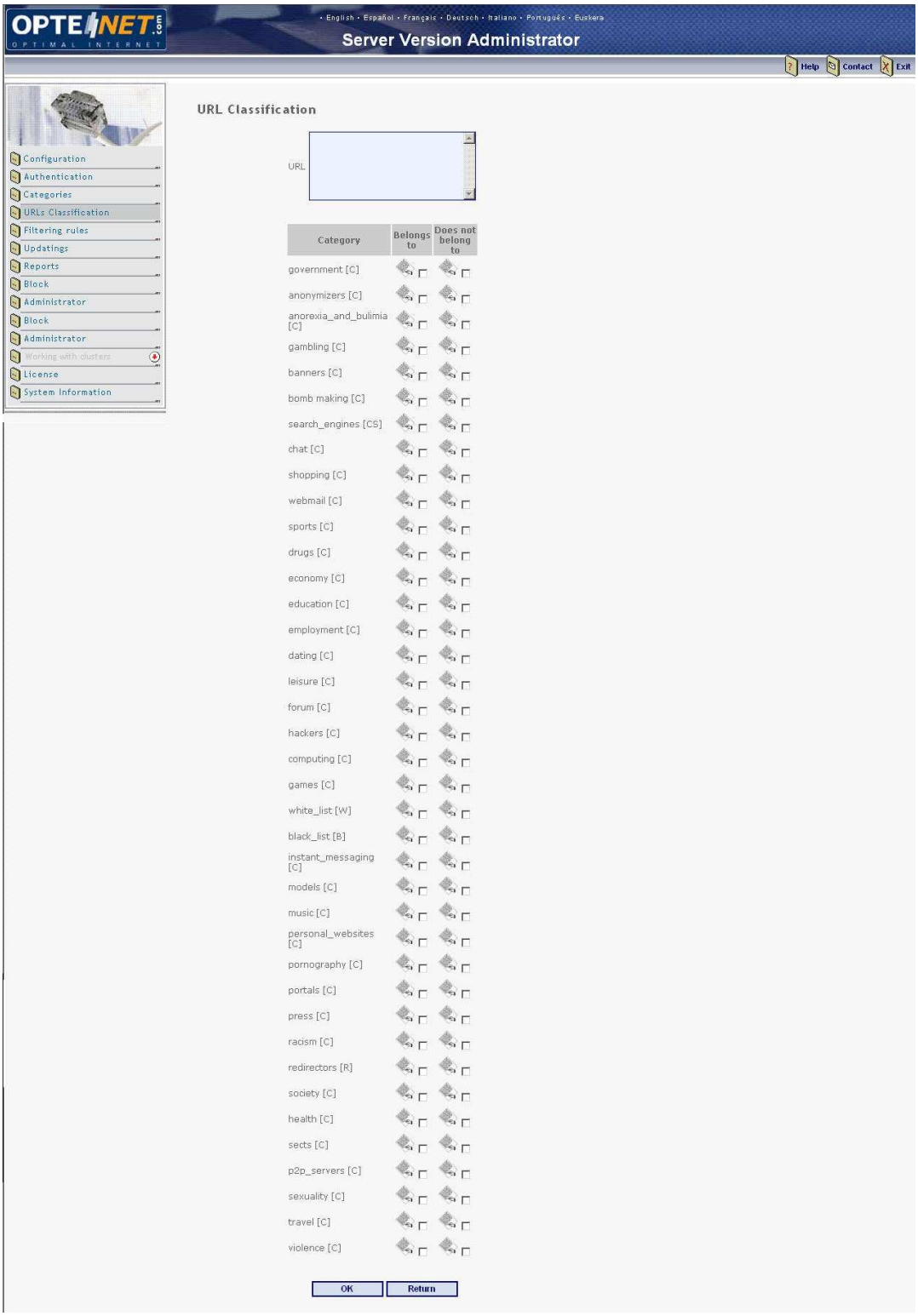
5.6. URL classification

In this option, we can add URLs to the various categories by indicating if a particular URL does or does not belong to a category.

This option is very useful when unblocking URLs that OPTENET associates with a certain category but which the administrator considers should not belong to that category.

The category type is shown alongside its name:

- C: content category.
- W: white category.
- B: black category.
- S: searchers categrory.
- R: remailers category.



From this screen, a URL can be inserted in various categories at the same time. This can happen because the categories are not exclusive sets. For example, sports press is categorised as press and as sports at the same time. The precedence of these user lists is greater than the lists predefined by OPTENET, thereby allowing the URLs that OPTENET filters to be unblocked and allowing the URLs that OPTENET does not block to be blocked.

It is possible to indicate that a single page does or does not belong to a category by entering a complete URL, for example,

http://www.dangerousplace.com/index.htm

or, on the other hand, to indicate that an entire website does or does not belong to a category by indicating it with an * at the end, for example,

http://www.dangerousplace.com/*

It is also possible to use the asterisk as a wild card at the beginning and in the middle of a URL. In this way, we can indicate all hosts belonging to an organisation belong to a certain category, e.g.
http://*.dangerousplace.com*

In the case of remailer type categories, URL extraction patterns may be added, for example,

http://www.google.com/search?q=cache:*:#+

where the'#' indicates the point where the URL towards which is being redirected appears. The asterisk can also be used for URLs belonging to the remailers category.

It is important to remember that OPTENET works internally by using URLs without protocol (http, https, …).
In this respect, by introducing http://www.example.com in pornography, the following URL's will be categorized under pornography:
http://www.example.com
https://www.example.com
ftp://www.example.com

By clicking on the icon to the right of each category, you can edit the list of URLs that you have been adding to this category. This list is presented in alphabetical order to make it easier to locate specific elements. From the next screen, you can add new URLs to the list of those that belong to a category or delete any if you have entered one by mistake, or delete all the URLs introduced into this category. In addition, the list of the URLs that do not belong to a category can be edited.

OPTENET
OPTIMAL INTERNET
English · Español · Français · Deutsch · Italiano · Português · Euskera
Server Version Administrator
Help
Contact
Configuration
Authentication
Categories
URLs Classification
URLs Classification
Filtering rules
Updatings
Block
Administrator
Gestion en grappe
System Information
URLs Yes
Rule DenyPorn
On this page you can add, remove and modify the URLs this rule will allow. A URL Yes is a URL this rule will always allow. You can allow a complete web site by placing an * at the end, for example, http://www.website.com/* or part of a place like http://www.website.com/part1/*. In order to include several URLs at the same time, each of them must be on a different line.
URL Yes
Add
Delete
URLs Yes Inserted
http://www.whitehouse.com/*
Return

Moreover, on this screen it is possible to enquire as to which categories apply to a particular URL. With this function it is very easy to avoid inserting URLs into a particular category when they already fall into it.

To this end, the user has to enter the URL into the text box and click the “Look Up” button. Immediately the list of categories that apply to the specified URL appears below the text box. If no categories apply, the message “No categories apply” appears.

5.7. Filtering Rules

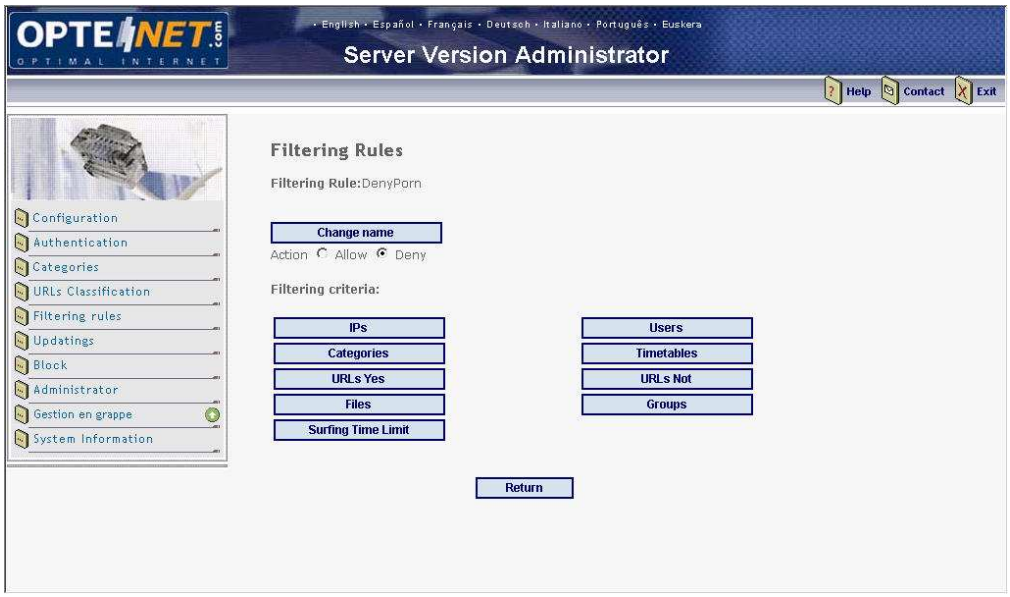
With the filtering rules, and as explained in section 4.5 of this document, we can easily personalise OPTENET Server in order to adapt it to the needs of our network.

In this option, you can define these rules and all of their criteria: IP Groups, Users, User Groups, Categories, URLs, Files and time schedules.

You must keep in mind that in the event of conflict between the rules, their precedence is taken into account. In other words, when analysing whether or not a request must be blocked, more than one rule may apply to that request (because the user is included in more than one rule), and the rule that decides is the one that appears first in the order of precedence.

After the Filtering Rules option has been selected, the next window appears where we can see all of the rules that we have defined on the system and their order of precedence.

From here, we can create a new rule, modify or delete an existing one and change their order of precedence and see a summary of what that rule contains. To do so, we simply have to select the rule that we want to modify and click on the corresponding button. We then obtain another window that shows the name of the selected rule and the operations that we can perform.



5.7.1. Change Name

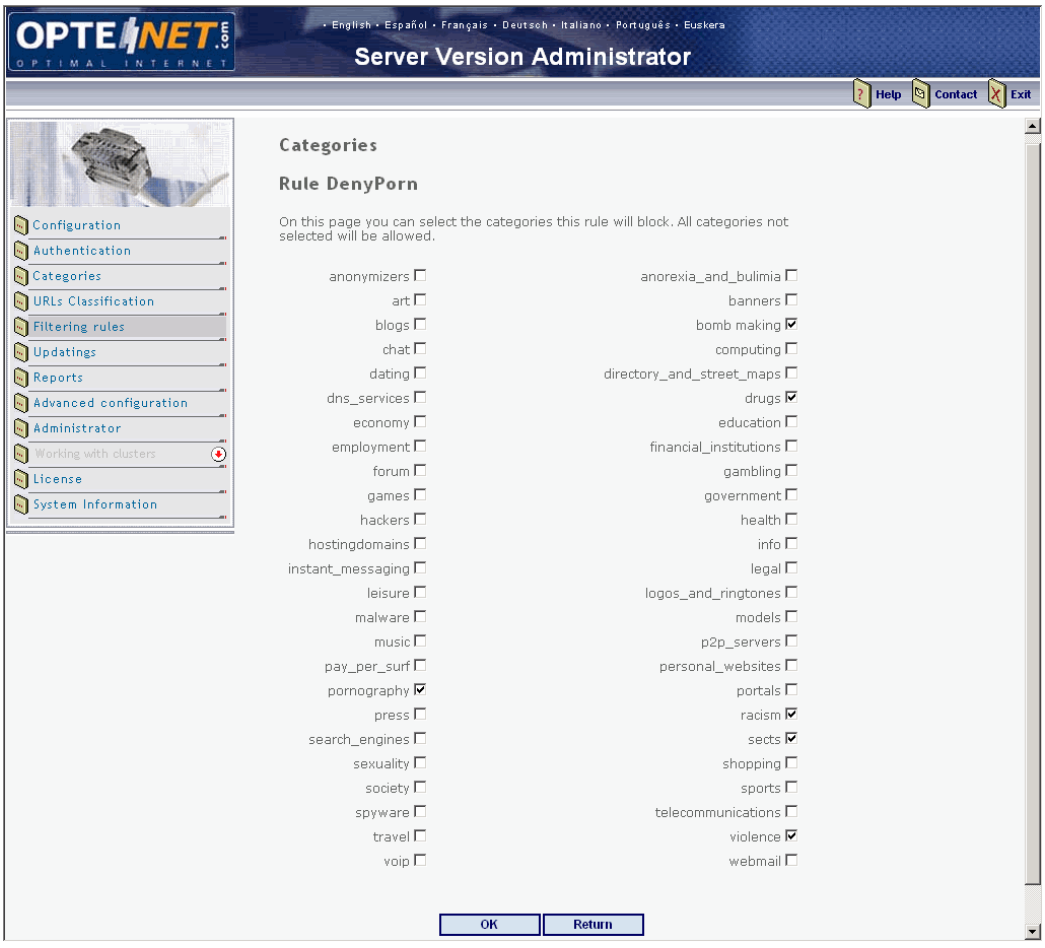
From this option, we can change the name of the rule. By default, when a new rule is created, it appears with the name, Rnumber. Through this option, we can give a significant name to the rule.

5.7.2. Action

The action indicates if this rule will be to allow or to deny the accesses to the categories that are selected in this rule. This option is selected from the main Window for Modification of a Filtering Rule.

5.7.3. Categories

In this option, you can select the content Categories to which the rule is applied. Only the categories amongst which the contents are included will be shown.

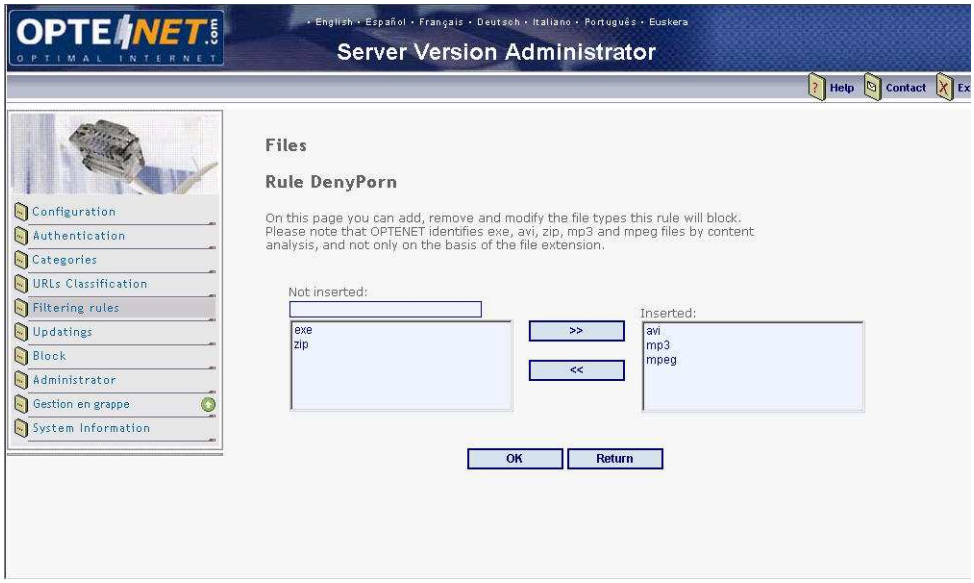


It is also possible to create rules that apply to all requests that the filter system is unable to categorise because the requested URL does not fall into any of the categories supported by the tool. To achieve this, the user only has to tick the option “Apply to uncategorised requests (other)”. This option can be selected in conjunction with other categories. So, for example, if this option is ticked as well as the pornography option the rule will be applied to all requests that are in the pornography category and furthermore to all those that are not associated with any category.

5.7.4. Files

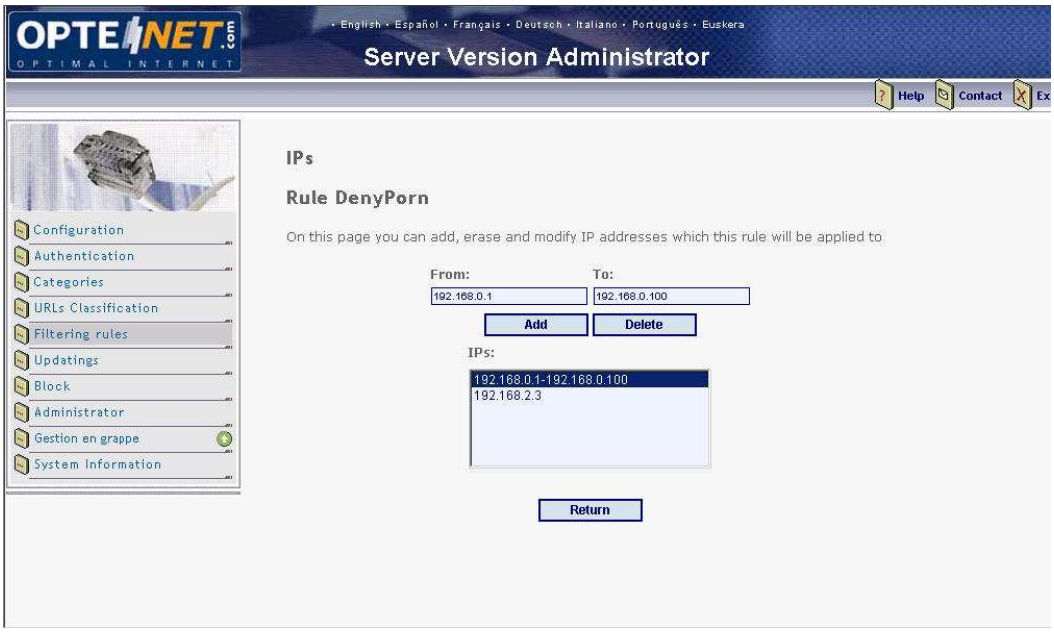
In this section, you can select the file types that will be subject to the Rule. If no files are selected, the rule will not take them into account, OPTENET identifies the types of file displayed in the left hand column (avi, exe, Mp3, mpeg, zip) by analysing the contents of the file. It can detect the many renamed files that are on the Internet, to prevent filtering by extension. As well as these types of files, it is also possible to include other different ones, writing there extension in the text box “not included” and then clicking on the button “>>”. These types of files will be filtered solely extracting the extension of the file that is being downloaded.

This feature distinguishes OPTENET from other filtering systems, it is able to perform the feature because it also analyses the contents of the file that is downloaded from the Internet.



5.7.5. IPs

In this option, we can define customer IP groups on which the selected rule is going to act.



For this option, we must take into account the following: if we do not indicate an IP, then this rule will act on all requests that reach it from any IP. If an address is indicated, then the rule is only applied to the requests that reach it from that address or those client IPs. For the rest of the requests, this rule is not considered applicable.

It is possible to indicate single IPs by simply entering the IP in the **From:** field, or to indicate a range of IPs by entering the initial IP in the **From:** field and the final IP in the **To:** field.

5.7.6. Users

In this option, you will be able to add and delete the users to whom the rule will be applied.

In order to establish rules by users you must configure your proxy or appliance to carry out the user authentication or force OPTENET to perform the authentication, by activating the “activate authentication” option in the configuration section.

In order for the users of your LDAP, Windows NT Domain OPTENET proxy or NCSA from SQUID server to appear in the list of those not included, you must first have configured the server in the “authentication” option. By clicking on “Refresh”, all users will appear. If none appear, the reason why the users could not be obtained from the server will be displayed in the system’s syslog (/var/log/messages file on Linux or /var/adm/messages on Solaris or Aix) or in the Windows Event Viewer.

As with the IPs, if we do not indicate any users, then this rule will be applied to all of them; however, if we indicate some, then the rule will only be applied to the selected users.

5.7.7. User groups

In this option, you will be able to add and delete User Groups to which the rule will be applied. In order for the groups of a certain LDAP or Windows Domain server to appear on the list of those not included, the server first has to be configured from the "authentication" option and you must then click on “Refresh”.

If users are indicated individually in the rule, and user groups are also indicated, then that rule will be applied to a user if that user is on the list of users entered in the rule or if any of the groups to which that user belongs is on the list of groups to which the rule must be applied. Please consider what is explained in the section “5.4. User authentication” if you want to associate groups of users to the filtering rules.

5.7.8. Surfing Time Limit

In this option, you can include the maximum number of hours per day that users can surf the Internet in the selected rule. You can also cancel the option by clicking on Clear.

5.7.9. Time Schedules

In this option, you will be able to add, delete and change the days of the week and the time intervals as the criteria of a rule. Outside the indicated intervals the rule will have no effect. If no interval is indicated the rule will be applied 24 hours a day, 7 days a week.

5.7.10. URLs Yes

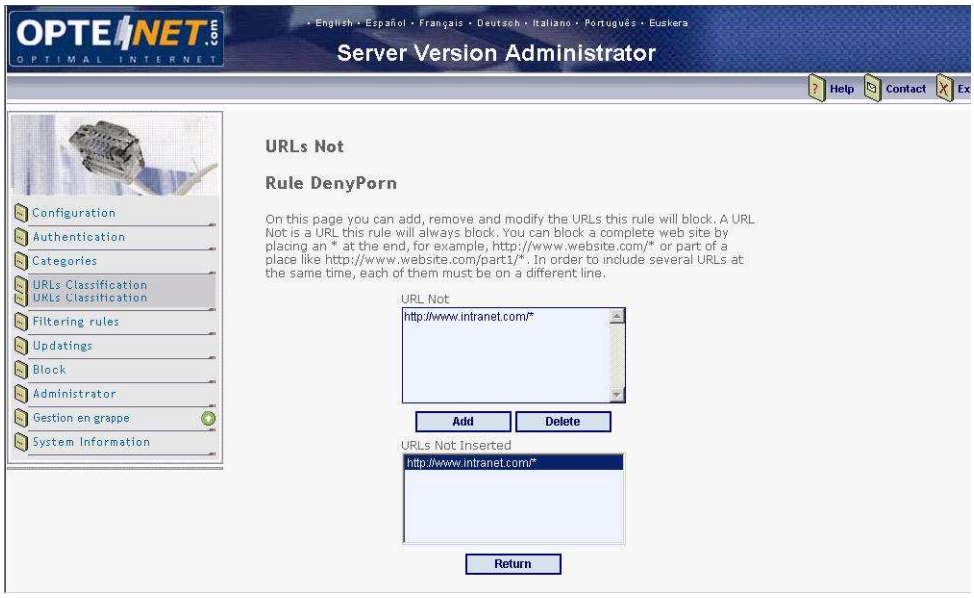
In this option, you will be able to add, delete and modify Yes URLs as the criteria of a rule. The Yes list contains the URLs to which the rule must be applied, regardless of their category and the type of file, therefore, if the rest of the characteristics are met (day and time and user, group or IP), then the rule will carry out its action. If the rule's action is to allow, then these URLs will be explicitly allowed. If, on the other hand, the rule's action is to deny, then these URLs will be blocked.

It is possible to indicate an entire site by putting an * at the end. It is also possible to use the asterisk as a wild card at the beginning or in the middle of the URL.

OPTENET
English · Español · Français · Deutsch · Italiano · Português · Euskera
Server Version Administrator
Help
Contact
Configuration
Authentication
Categories
URLs Classification
URLs Classification
Filtering rules
Updatings
Block
Administrator
Gestion en grappe
System Information
URLs Yes
Rule DenyPorn
On this page you can add, remove and modify the URLs this rule will allow. A URL Yes is a URL this rule will always allow. You can allow a complete web site by placing an * at the end, for example, http://www.website.com/* or part of a place like http://www.website.com/part1/*. In order to include several URLs at the same time, each of them must be on a different line.
URL Yes
http://www.whitehouse.com/*
Add
Delete
URLs Yes Inserted
http://www.whitehouse.com/*
Return

5.7.11. URLs Not

In this option, you will be able to add, delete and modify Not URLs as the criteria of a rule.


OPTENET
OPTIMAL INTERNET
English · Español · Français · Deutsch · Italiano · Português · Euskera
Server Version Administrator
Help
Contact
Configuration
Authentication
Categories
URLs Classification
URLs Classification
Filtering rules
Updatings
Block
Administrator
Gestion en grappe
System Information
URLs Not
Rule DenyPorn
On this page you can add, remove and modify the URLs this rule will block. A URL Not is a URL this rule will always block. You can block a complete web site by placing an * at the end, for example, http://www.website.com/* or part of a place like http://www.website.com/part1/* . In order to include several URLs at the same time, each of them must be on a different line.
URL Not
http://www.intranet.com/*
Add
Delete
URLs Not Inserted
http://www.intranet.com/*
Return

The Not list contains the URLs to which the rule must never be applied, which means the exceptions to the rule. It is possible to indicate an entire site by putting an * at the end. It is also possible to use the asterisk as a wild card at the beginning or in the middle of the URL.

5.7.12. Example of rule use

We will now use some simple examples to see how the rules work.

By default, when OPTENET is installed there is only one rule, DenyPorn, which blocks access to sites with pornographic content. Let's see how this rule is configured. In the category option, this rule has the basic filtering categories marked: pornography, racism, violence, sects, drugs and the construction of explosives, meaning that this rule blocks these five categories. Who is prohibited from this content? If we look at the users, we see that there are no users defined, and therefore it affects all users. The same thing happens with the user groups. Which machine? There also are no IP addresses defined, and therefore this rule is applicable to all of the,. During what time schedules? Since none is specified, it is applicable at all times of the day. Is there any exception to this rule? We see that there are no addresses on either the Yes URL list (the URLs that directly meet this rule) or the Not URL list (URLs that never meet this rule), which means that there are no exceptions to this rule.

In summary, by default when the filter is installed, access is blocked to the aforementioned content for all users and machines that surf via the proxy.

5.7.12.1. Rule for the manager

Now let's Imagine that the manager requires access without filters. This means that the manager must not be affected by any filtering rule. The solution is easy. We will create a rule for the manager where, in users, we include the user id which is used to authenticate the manager, or if there is no user authentication, in the IP section we will include the IP of his or her machine. Then we will set the action of the rule as "Allow," and we will not

select any categories. In other words, we have created a rule that is only applicable to the manager and which is to allow. Allow what? Since we have not selected any categories or file types, it will allow everything. When? Since we have not selected any time or day, it will always be allowed.

One detail remains: we must give this rule the highest priority rule. Therefore, when the manager surfs the Internet, OPTENET will analyse his or her requests starting from the highest priority rule. It will see that the requests meet that rule and will allow access to all contents.

5.7.12.2. Rule to block press and sports during work hours

Another example: suppose that we now want to block access to sports and press content during work hours (from 9:00 to 14:00 and from 16:00 to 19:00), Monday to Friday. It's easy: we create a new rule called PressOnJob and make the time schedule from 9:00 to 14.00 and 16:00 to 19:00, Monday to Friday. The categories that this rule filters are Press and Sports.

What position should we give it? We must think about which of the three rules that we have up to now is the most general, and put it at the end, and then go up in hierarchy to the most specific. Therefore, DenyPorn is the most general, which inhibits pornography, PressOnJob would be next, followed by the manager rule.

Could we also have included the DenyPorn rule in the Press and Sports categories and have marked the working hours as the time schedule? The answer is no. If we do not create a new rule, and instead we modify DenyPorn by adding more categories and modifying its time schedule, we are making it possible to also access pornographic content outside of this time schedule (after 19:00).

5.8. Updates

OPTENET Server connects continuously to the different list updaters to update its lists incrementally so as to be able to filter the new, categorised Internet addresses that arise every day. All the URLs added are stored in memory and must be written to disk periodically.
The following parameters can be configured from this option.

5.8.1. Via proxy

Select this option if the server where OPTENET is installed cannot access Internet directly and needs to do so via a proxy. Indicate the IP address of the proxy (or its name) and port. Ensure that this proxy does not request authentication from OPTENET requests.

5.8.2. Updating Frequency

OPTENET requests the new URL's that are incrementally categorised and pieces of several Kbytes so as not to congest the network traffic. The time between consecutive updates indicates the seconds that OPTENET waits between two consecutive updates, supposing that it has new URL's to update. The time between checks indicates the seconds that OPTENET waits when it is fully updated before performing the next check.
The default values (30 and 300 seconds) are designed so that the unblockings may be requested from the blocking page arrive at the filter in a brief period of time.

5.8.3. Consolidation to disk

The new addresses received by the filter are stored in memory for efficiency reasons and are saved to disk in the consolidation process. This process may be programmed daily, weekly or monthly by indicating the interval period at the starting time. OPTENET recommends daily saving to disk timed to coincide with the periods of least activity in the network, which normally occur at night.

5.8.4. Absolute reloading of listings

It is possible to perform a compete reloading of lists at the current instant by only clicking on the button "Reload now" located in the lower part of the window. Once the reloading process is launched, you will be able to monitor how the reloading evolves from the section "System information" where the bytes downloaded will be indicated as web as the totals and result of the reloading.

5.9. Reports

When you click on this option, another browser window opens connected to OPTENET Reporter. OPTENET Reporter is the tool that enables you to extract reports on Internet use. By default it can be installed with OPTENET Server as they are distributed together.
If when you click on this option OPTENET Reporter is not running, a message appears indicating that it is not possible to contact the reporting tool. Please check that OPTENET Reporter is running and that it is installed on the machine's IP and listening at the right port. By default, OPTENET Server tries to contact an OPTENET Reporter installed on the same server.

Once OPTENET Reporter has started up and you have ensured that its IP and administration port are properly configured in the right section of OPTENET Server, click on the "Reports" option again and OPTENET Reporter administration will open in a new browser window.

5.10. Administrator Identification

OPTENET Server establishes a number of levels of administration as the following table shows:

	Administrator	Local Administrator	URLs and categories Administrator	Reports Operator
Introduction	X	X	X	X
Documentation	X	X	X	X
Configuration	X			
Authentication	X			
Activate authentication	X			
Type of authentication	X			
Categories	X	X	X	
URLs classification	X			
Display	X	X	X	
Add	X	X	X	
Remove	X	X	X	
Filtering rules	X			
Delete	X			
Add	X			
Modify	X			
Modify URL's and categories associated with a rule	X		X	
Updates	X			
Block	X	X		
Reports	X	X		X
Administrator	X	X		
Administrators	X			
Local Administrators	X	X		
URLs & categories Operators	X	X		
Reports Operators	X	X		
Cluster management	X			
License				
System Information	X	X		X
Obtain logs for the report generator				X

By default, after installation one user exists for each profile, but only the "Administrator" and "Information_Operator" levels are activated. The Administrator profile has total control over the filter and can carry out all administration operations, except inserting and deleting users belonging to the "Reports Operator" profile, and therefore it cannot manage the sensitive information password. By default, the administration username is **optenet** and the password is **12345678**. These values can be changed from the WWW administration using the menu option Administrator. It is advisable to change them as soon as OPTENET Server is installed.

The data of the default users that are present in the installation can be modified for each profile and new users can be added or deleted as required. To do this click on Administrator and you will be shown a list of all users grouped by profile. You must then select the user to delete or modify and click on the corresponding button, or simply click on “New” if you wish to create a new user.

To activate other update levels, click on the button of the required level. On the next screen, activate the “activate profile” option, enter the username and password, and then click on OK as shown below:

The sensitive information password deserves a special mention. OPTENET server stores the personal information about the user who is surfing in its logs in encrypted form. A double password is therefore required to decrypt it. This information is displayed in the report module. A first password is required to access the report module. Once you are inside the report module, you will need to enter a the user information’s password to view the sensitive information. This password should be entered in the password box in the menu Configuration → Options.

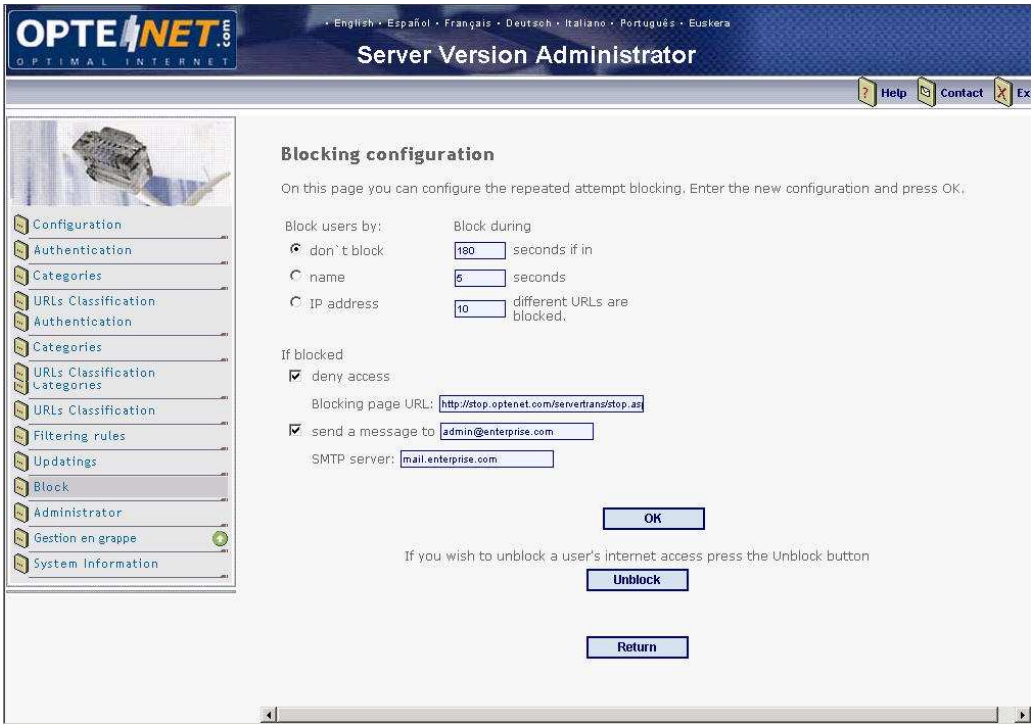
5.11. Advanced configuration

This screen allows the administrator to carry out a series of advanced actions, in order to customise specific filtering characteristics. Amongst the options available, they can:

- Configure blocks for repeated attempts.
- Configure filters for Skype instant messaging services.
- Dump navigation logs generated by OPTENET.

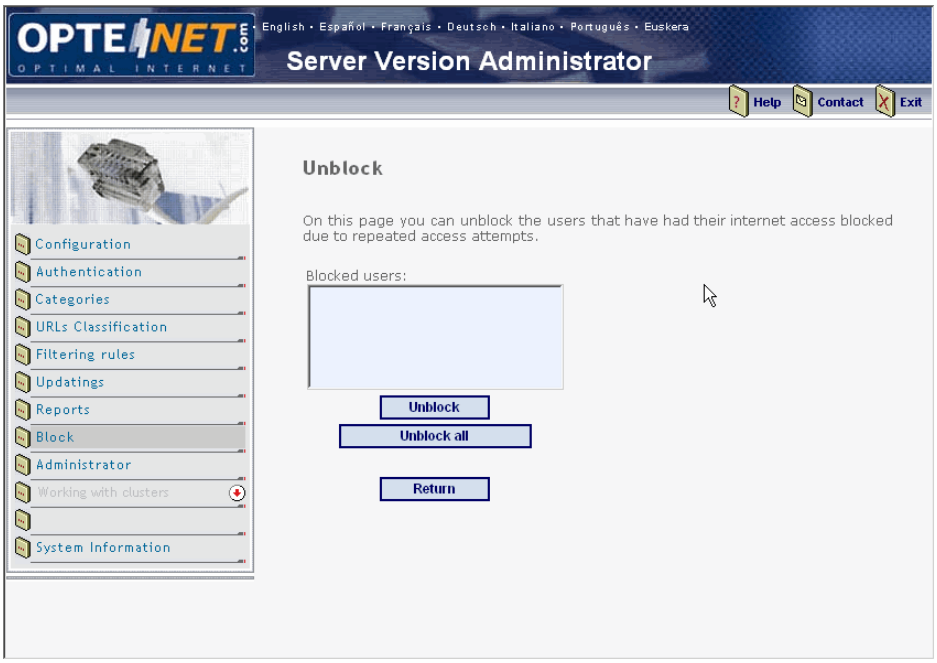
5.11.1. Configuration of repeated attempt blocks

With this new characteristic you can completely block access to the Internet for one user that has tried to access more than a certain number of forbidden sites in a certain period of time. The aim of this functionality is to enable the penalisation of users who try to get passed the filter.



By default, this option is deactivated, to activate it simply select whether the users are identified by name (user authentication) or by IP, the time they will be blocked as penalisation and the number of blocks they are allowed to have in a certain period of time. In addition, in the event of a block you can configure the blocking page that should be shown and the possibility of sending an e-mail to the system administrator notifying this situation.

If you want to unblock a user that has been blocked for this reason, you can do so from the following screen that appears when you press the Unblock button.



This screen will show a list featuring all the users that are currently blocked. A specific user can be unblocked by selecting same and clicking on the button ‘Unblock’. All the users can be unblocked by simply clicking on the button ‘Unblock All’.

5.11.2. Skype detection

Skype is a well-known instant messaging application that allows users to make phone calls over the internet or to use chats, file transfers, etc.

The most unusual feature of this application is that it does not use a series of predefined ports to establish communication between different users, instead, if the default ports are not available, it then uses the ports used for HTTP (80) and HTTPS (443) communications.

This means that Skype users can overcome limits set in firewalls, as these work by blocking outgoing and incoming communication on certain given ports. Thus, blocking access to these ports is not sufficient to stop the organisation’s users from using the Skype service.

Additionally, Skype encrypts all that transmitted with a proprietary algorithm before sending it over the internet, which means that it is even more difficult to identify data packets coming from Skype clients.

OPTENET uses communication analysis to detect possible Skype communication; thus all packets that are suspected of containing Skype messages are analysed, determining whether any given node uses the HTTP or HTTPS ports for this type of communication.

A screen like the one below appears on accessing Skype detection configuration:

Here is a breakdown of each of the available options.

5.11.2.1. Enabling Skype detection

By default, the Skype detection option is disabled. To enable it, simply check the corresponding option. The rest of the configuration parameters only take effect when this option is enabled. Likewise, the Skype detection option is only currently available for integrations with ICAP systems.

5.11.2.2. Maximum number of simultaneous connections

To carry out Skype traffic detection, OPTENET analyses messages suspected of belonging to Skype communications.

During the analysis, the ICAP thread managing the request remains occupied. Defining this parameter allows for the limitation of the number of simultaneous ICAP threads to be used for Skype detection, to ensure that there always some threads reserved for traditional navigation.

Correctly defining this parameter is very important given that traditional Skype clients, when connecting, make multiple requests simultaneously to the numerous Skype servers available. If Skype detections are allowed to consume all the ICAP connections available, the internet service will be out of action during the time the Skype analysis takes. Thus, it is advisable to assign a value equal to or lower than 50% of the total number of ICAP threads enabled.

5.11.2.3. Time to live for nodes detected as Skype

When a node is detected as Skype by OPTENET, then it is saved in an internal cache so as to ensure that future requests to analyse this node again are avoided. Entries in this cache are given a set time to live, as defined in this section. The minimum time to live for an entry in this cache is 3600 seconds.

The administrator may want entries in the cache never to expire. This can be achieved by entering the value zero in the corresponding box. Thus, entries remain in the cache and are applied permanently.

5.11.2.4. Timeout for Skype detection connections

To carry out Skype detection, a series of connections are made to possible Skype nodes. It may be that these connections are rejected, as with any other kind of connection. The time that OPTENET spends waiting for a response from the server to be tested can be set in this section. The default setting is 10 seconds.

5.11.2.5. Enabling detection on ports

OPTENET allows the administrator to set the ports that are to be tested for Skype patterns. It is possible to enable detection on ports 80 and 443 separately. This means that a user can decide to test communications addressed to port 80 only, those using port 443, or both.

If Skype detection is enabled, at least one of these ports has to be enabled. Even so, it is advisable for detection to be carried on both, as Skype clients use both indistinctly for communications.

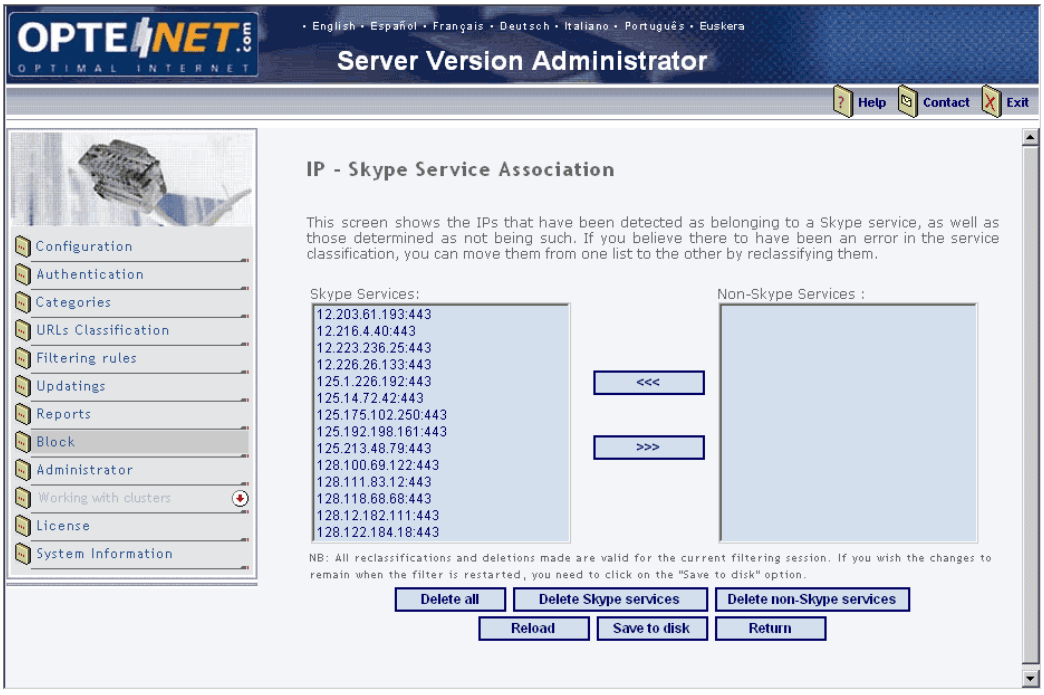
5.11.2.6. Operating policies

OPTENET allows the administrator to define the different operating policies, offering them the option of deciding what action is to be taken in certain cases during Skype detection. The policies that can be set by the administrator are:

- Blocking those requests that cannot be analysed due to the maximum number of simultaneous connections having been reached: when a request that is a candidate for containing Skype traffic cannot be analysed because all the threads for detection are in use, the administrator can set whether or not they want this request blocked. Whatever the case, this will never be included in the internal cache, which means if an identical request arrives and threads are available, it will be analysed. This is enabled by default.
- Blocking new requests addressed to sites that are currently being analysed: when a request arrives for a node that is already being analysed, this new request can be analysed as well or blocked temporarily. These requests are blocked by default, as, if not, the detection threads would soon become overloaded.
- Blocking those requests that can be checked by a connection timeout: when a request to a node suspected of being Skype is analysed, this node may not respond within the time limit set by the administrator. If this connection time runs out, the administrator can decide to block or allow the request. The option to block the request is enabled by default.
- Including entries that have been determined as not being Skype traffic in the Skype cache: when Skype detection has been carried out, the analysis may determine that a given node does not contain Skype traffic. The administrator can decide whether these entries should be included or not in the Skype nodes internal cache - which means that those that are not included, if a new request arrives, will be analysed again. This option is enabled by default.

5.11.2.7. Management of the Skype detection cache

Additionally, the administrator can mange the Skype detection cache. To do so, they have to click on the “View cache” button. A screen like that below will appear:



This screen shows two lists. The list on the left contains all those nodes that have been detected as belonging to Skype communications and whose time to live has yet to expire. The list on the right shows all those nodes that have been determined as not belonging to Skype communications.

The administrator can pass nodes from one list to the other by selecting an entry from one of them and clicking on the corresponding button. Likewise, they can delete entries from the Skype node list, non-Skype node list, or indeed all the entries in the cache.

All these operations are carried out for the current OPTENET session, which means that if the changes are to be maintained for futures sessions (for example, if the filter is reset), then the administrator has to click on the “Save to disk” button. Likewise, the administrator can reload the list at any time, as there may be updates if detection has been enabled.

5.11.3. Log dump

OPTENET does not write entries in the navigation logs generated directly on to the disk, instead storing these entries internally to subsequently write them all together in one go. This makes the log writing process more efficient. When the space used for temporary storage runs out or when a period of time passes without writing to the disk, OPTENET dumps the data stored automatically.

This option allows the administrator to carry out a dump immediately for the entries pending writing to the disk.

5.12. Cluster management

This version of OPTENET Server allows multiples instances* of OPTENET Server to be handled from only one WWW server. This way of working is called ‘Cluster management’.

Once the OPTENET Server instances have been defined as described under the following headings, each change applied to OPTENET Server, will be copied to all the instances automatically.

If OPTENET Server cannot connect with one or several of the instances, it will then show the following warning message with the lsit of instances where the change cannot be applied.

* An instance is understood to be an installation of OPTENET Server that is being run on a machine.

5.12.1. Activate/Deactivate Cluster management

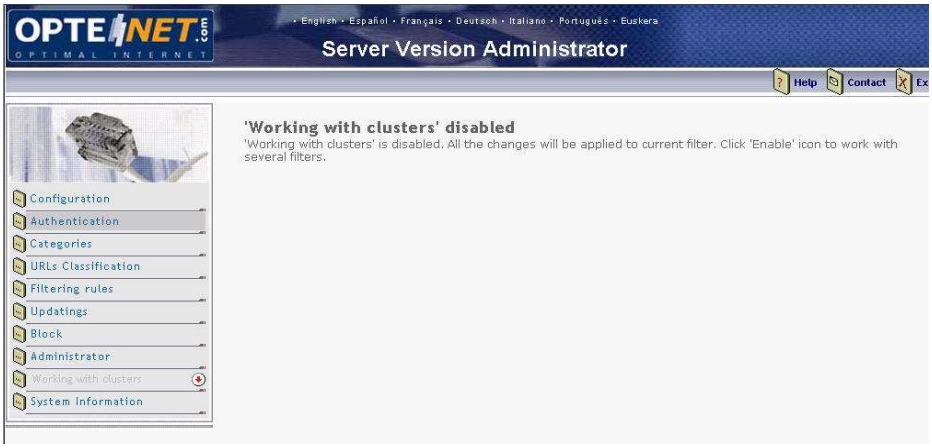
The most important element in Cluster management, is the icon located in the bottom left-hand part of the screen and it serves to activate or deactivate the Cluster management option.

OPTENET
OPTIMAL INTERNET
· English · Español · Français · Deutsch · Italiano · Português · Euskera
Server Version Administrator
Help
Contact
Exit
Configuration
Authentication
Categories
URLs Classification
Filtering rules
Updatings
Reports
Block
Administrator
Working with clusters
License
System Information
Introduction
OPTENET is a powerful filtering system that enables your company to optimize Internet resources - both the content served and the time spent. Its leading Internet access filtering technology permits maximum control over your employees' Internet use.
To do that OPTENET has four filtering levels:
Filtering based on semantic analysis of the text of the web page. OPTENET analyzes each web page at download time from the Internet allowing a higher lever of security.
Filtering based on predefined lists consisting of manually revised addresses.
Filtering based on URL analysis
Filtering based on administrator defined lists.
OPTENET Server Version also has the following features:
Automatically updated lists.
User customizable lists.
Administration via WWW.

When it is deactivated, it works in conventional way, which means that only one OPTENET Server is handled and the changes are only applied to the installation that is being administered. When it is activated, all the changes that are made in the configuration of this filter answer all installations of OPTENET Server that are configured within the Cluster management option.

In the configuration and updating screens a message will be shown indicating that these changes will affect all OPTENET Server installations. For the other options no message will be shown.

When Cluster management is activated, it shows the screen where it is able to edit the installations of OPTENET Server. In addition, the “Cluster management” button is activated and the icon that shows the working mode (activated, deactivated) is updated.
When Cluster management is deactivated, the following screen is shown which indicates that the working mode is traditional, and that the changes are only applied to one OPTENET Server. The “Cluster management” button and the icon have been updated again.



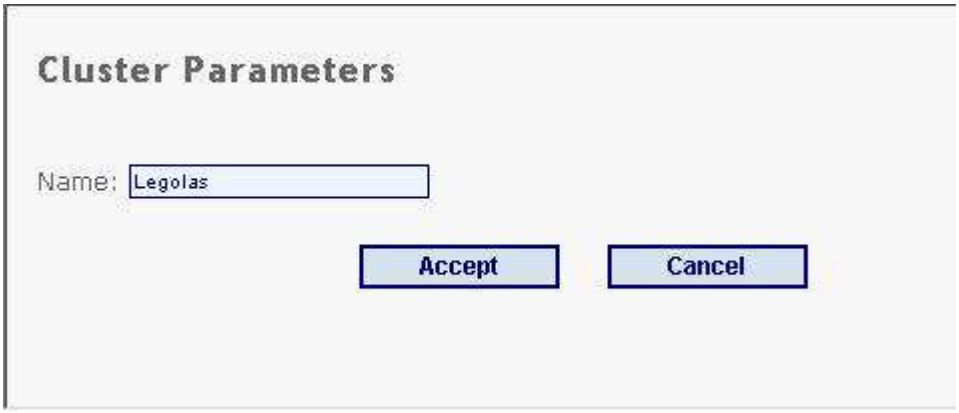
5.12.2. Clusters

He we can find the buttons to edit clusters and at all times an updated list is shown with the clusters created.

For all operations except “Insert” it is necessary to previously select the cluster.

5.12.2.1. New

To insert a new cluster the following window is shown:



You just have to enter the name and the cluster will be automatically shown on the list.

5.12.2.2. Edit

It allows you to edit the name of cluster. The same window is shown as in the previous operation but with the name of the cluster in the text box.

5.12.2.3. Delete

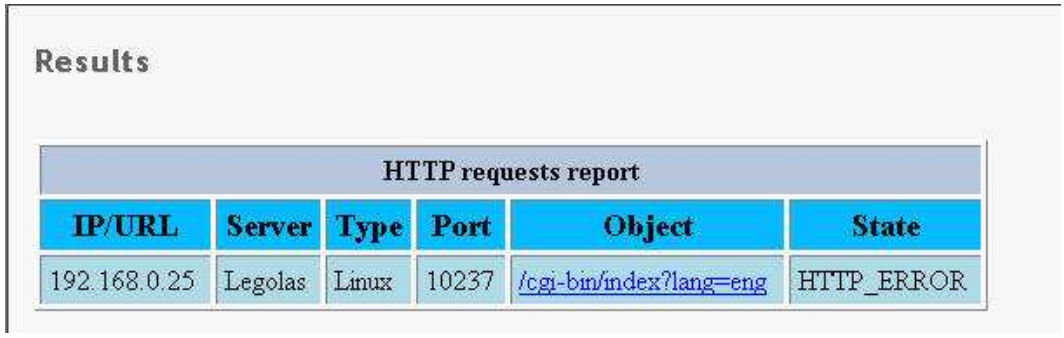
It permanently deletes the selected cluster from the list of clusters.

5.12.2.4. Connect

It establishes connections to all the servers of the selected cluster and shows the report window of the following section.

5.12.2.5. Report

It shows the result of the connections made to the servers in the following window.



The fields of the table are:
IP/URL: IP of the instance of OPTENET Server.
Server: Name of the server.
Type: Type of OPTENET Server.
Port: Port where the instance of OPTENET Server listens.
Object: The request that is made to the instance of OPTENET Server.
State: 'HTTP OK' (OPTENET Server is being run)
'HTTP_ERROR' (OPTENET Server is not being run or the parameters entered are incorrect).

5.12.3. Servers

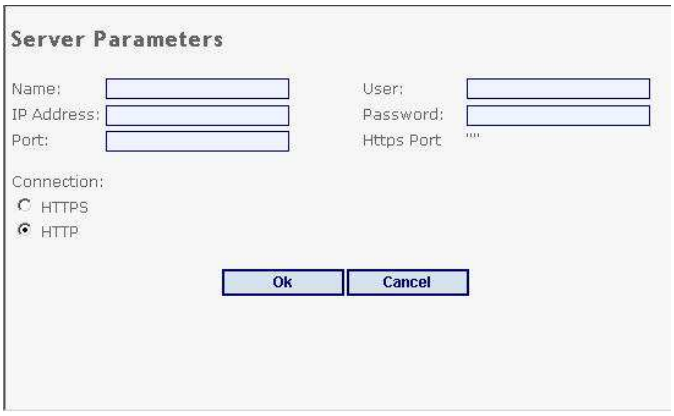
Here we have the buttons to edit servers.

At all times an updated list is shown with the servers entered for the selected cluster.

It is important to point out that the installation of OPTENET Server with the WWW administration we are connected to, must NOT be added (or inserted) to the list of servers, because the changes will always be applied to it, regardless of the working mode.

For all operations it is necessary to previously select the cluster. The server to edit will belong to this cluster. When selecting the cluster, all the servers who belong to this cluster will be shown.

In the text box, the following information is shown for each server: IP - Name - IP:Port - Type.



5.12.3.1. New

To insert a new server the following window is shown:

The parameters in order to create a new entry of an installation of OPTENET Server that we wish to control are as follow:
Dir. IP: IP Direction.
Name: Name of the instance.
Port: Listening port.
User: User name for the identification.
Password: User password.
Connection: Type of connection to manage the other installations. HTTP (by default) or HTTPS (secure connection).

In order to work with https secure connections, please consult appendix 1 “Administration of OPTENET Server through a secure connection”, as in this case the “Port” field you must then enter is not the port where the OPTENET Server is listening, but rather the port where the stunnel, which is associated to the OPTENET Server that you are entering, is listening. It is important not to confuse this stunnel with the stunnel associated to the local filter, as they are different. Finally select ‘HTTPS’ in the ‘Connection’ field instead of ‘HTTP’.

In the window the label ‘Port Https’ is shown. When inserting a server this label is empty. In later sections we will see what values it can take.

The username and password are the same as the ones entered when you accessed the OPTENET Server WWW administration.

It is important to note that if you edit the administrator name and password when working with clusters this change is replicated in all the installations.

You should also note that if you delete the administrator name and password entered when defining the server, these will stop working with the cluster management. This is because the name and password used by the cluster management to replicate a change to a given installation no longer exists in that installation. In this case you will need to edit the server parameters and enter a new name and password for the management to work again.
A different procedure would be to edit the user instead of delete and recreating it.

5.12.3.2. Edit

The same window as in the previous operation is shown but with the server parameters in the text boxes.

If you are working with HTTP, you will see that the value shown in the 'Port Https' label is the same as the one entered in 'Port'. This is because there is no port associated to https connections.

Nevertheless, if you are working with secure connections, you will see that a port has been assigned. OPTENET Server has searched for a free port in the system and has started a stunnel instance on the local machine, in order to be able to communicate in secure mode.

For each new server created, OPTENET Server will start a stunnel instance on its local machine.

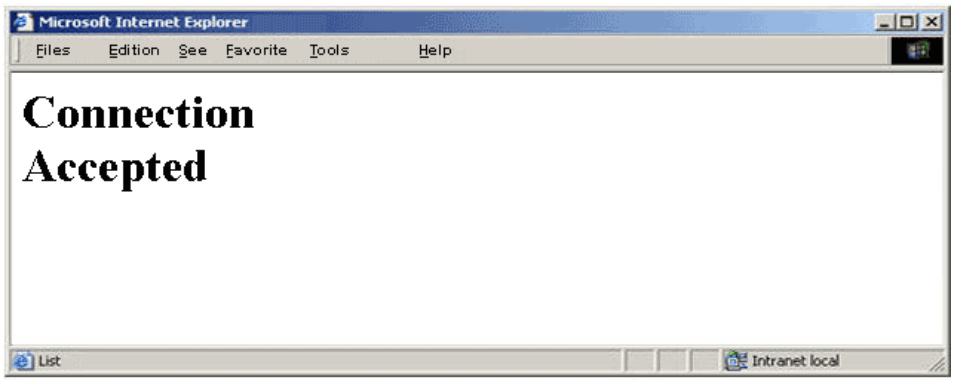
5.12.3.3. Delete

It permanently deletes the selected server from the list of servers.

If it you are working with secure connections, when a server is deleted, the instance of stunnel associated to this server that is on the local machine is also deleted.

5.12.3.4. Connect

It establishes a connection with the selected server and the following window is shown:



The result of the connection can be:
'Connection Accepted': OPTENET Server is being run.
'Error Connection not made': OPTENET Server is not being run or the parameters entered (user, password, dir. IP, etc.) are incorrect.

5.12.3.5. Report

The following window is shown with the result of the connection made to the server.
The table fields are the same as for the cluster reports.

5.13. License

If you have a license code that you could not register during the installation, you can register it at any time from the web administration (License option).

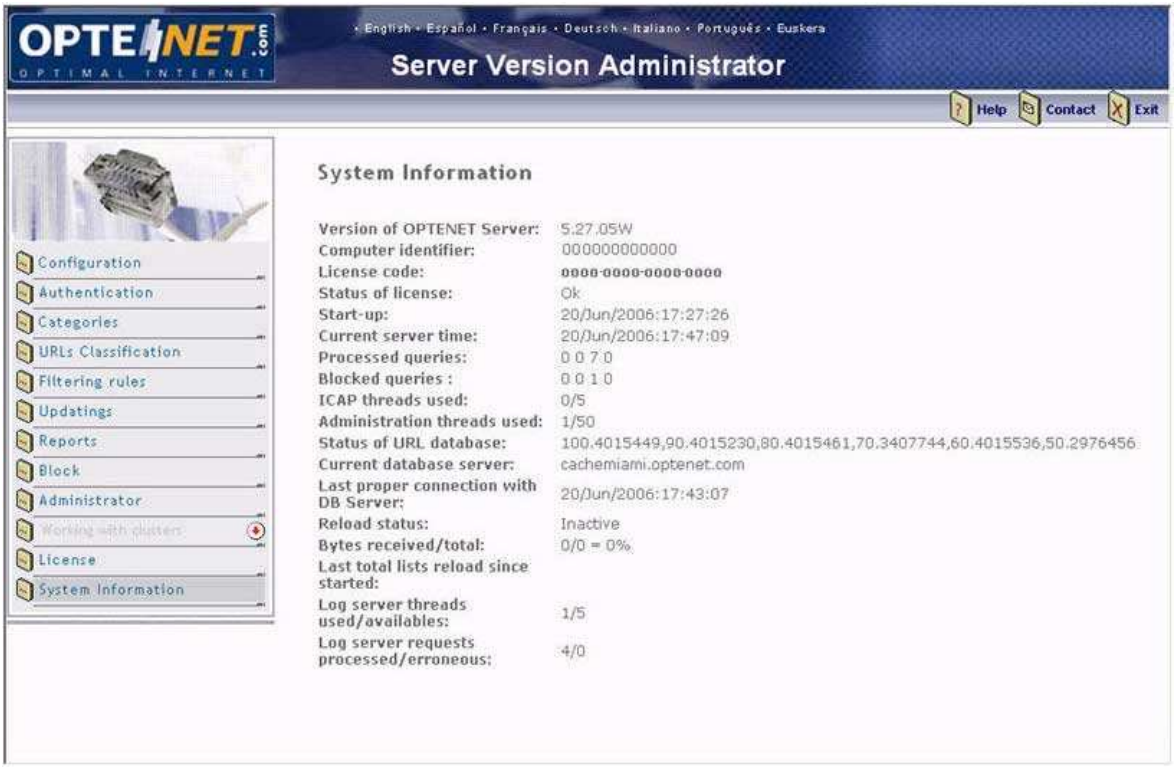
If the license in use has run out, in addition to registering a valid license, the filter must be restarted for the programme to operate correctly. If you are using a valid license and simply change to another one, you only have to introduce the new license and you will not have to restart the filter.

5.14. System information

The current state of the filter is shown in this option. There follows an explanation of the different sections on which information is shown:

- **Version:** the version of OPTENET Server running.
- **Computer ID:** the code identifying the computer for OPTENET programs.
- **License code:** the licence code used by the program.
- **License status:** this indicates the status of the licence. Should your licence expire, contact support@optenet.com to update it.
- **Start-up:** the date and time when the filter started up.
- **Current server time:** the date and time of the server running the filter.
- **Requests processed:** this indicates the total number of requests that the filter has received for analysis. It shows four numbers, the first indicates the ICAP REQMOD requests received for list checks, the second the ICAP RESPMOD requests received for content analysis, the third the requests received via RPC (SQUID, ISA Server, OPTENET Proxy, etc.) and the fourth the ICAP REQMOD_CATEGORY requests received.
- **Blocked requests:** this indicates the requests that have been blocked; it shows four numbers, which are the same as those used for requests processed.
- **ICAP threads:** the first number shows the ICAP server threads currently in use and the second the total number of ICAP server threads. These threads include all the possible ICAP services (reqmod, respmod and reqmod_category).
- **Administration threads**: the first number shows the web server threads currently in use and the second the total number of threads available. Bear in mind whether the local stop page serves this server.
- **Database status**: this is of no meaning to the user, but may be of use to OPTENET's technical staff.
- **Current database server:** this indicates which server is being used to update the URL database.

- **Last correct connection to the DB server:** the date and time of the last time the filter successfully contacted a URL database server.
- **Status of the last complete update:** this indicates the status of the last complete reloading of the URL database launched from the Updates section. Depending on the internet connection, a complete reload may take between a few seconds and a few minutes. The progress of this update can be monitored from here.
- **Bytes received/total:** this shows the bytes received for the complete reload and the total bytes that should be received, as well as the percentage completed.
- **Last correct update since start-up:** this indicates the date and time of the last successful complete update since the filter started up.
- **Log server threads**: the first number shows the threads used that are sending logs to an OPTENET Reporter and the second shows the total number of threads available.
- **Requests to the log server**: the first number shows the total number of successfully answered requests and the second the unsuccessful requests.

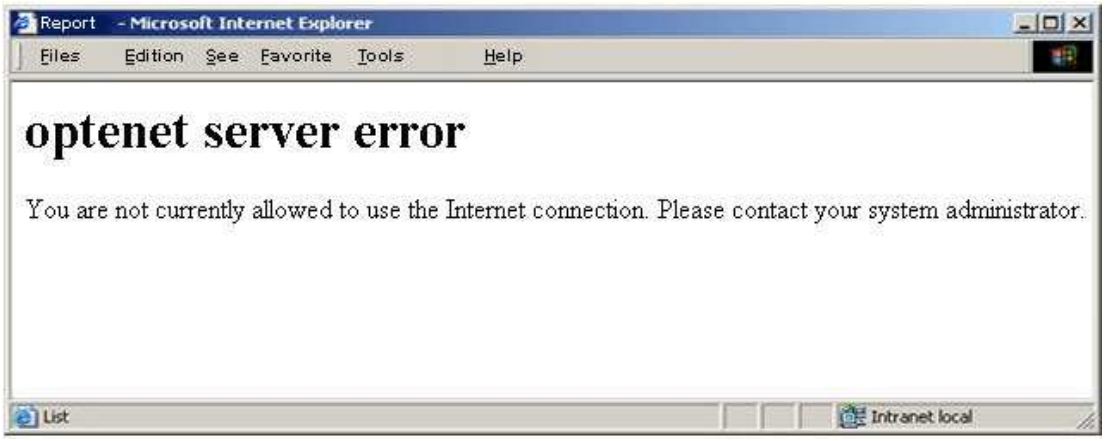


6. FREQUENT PROBLEMS

This section describes the most common problems and how to solve them.

6.1. The optenet server error message... appears when I try to surf

If the following screen appears when you attempt to surf while using the filter:


Report - Microsoft Internet Explorer
Files Edition See Favorite Tools Help
optenet server error
You are not currently allowed to use the Internet connection. Please contact your system administrator.
List
Intranet local

It is due to the fact that your OPTENET Server license has expired. Please contact us at on of the following:

support@optenet.com
+34 902 154 604 (Spain)
+34 913579150
+33 (0) 1 73 03 90 60 (France)
+44 (0) 870 099 0322 (United Kingdom)
+1 305 249 7505 (United States)

in order to renew your license or register.

6.2. The filter will not start

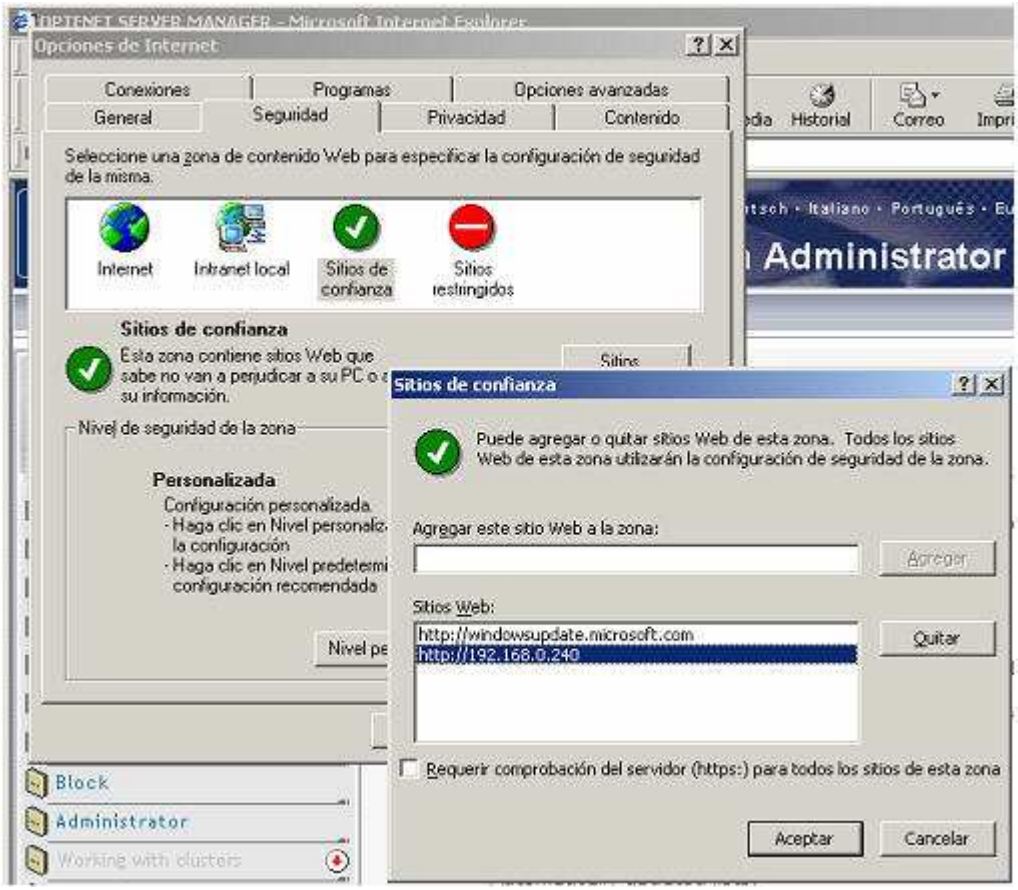
If the filter will not start operating when you attempt to start it, you can consult the reason in the system syslog. To do this you must connect as the root and view the last few lines of the/var/log/messages file on Linux or /var/adm/messages file on Solaris or Windows, or in the Windows event viewer.
OPTENET Server leaves an informative event every time it is started or states the problem found when it could not start.

6.3. The users do not appear when the refresh button is pressed

In order for the users to appear when the refresh button is pressed, the LDAP or Windows Domain server from which we are going to extract the users must first be defined. Be sure that this server is well defined and that it is accessible from the equipment where OPTENET Server is installed. Consult the system syslog (/var/log/messages file on Linux or /var/log/messages on Solaris or Aix or the Windows event viewer) in order to see the reason why OPTENET could not list those users.

6.4. I cannot enter the filter administration

We have been informed tht when Internet Explorer 6.0 is configured with a high securitylevel, the browser might show a blank page when the user name and password are introduced.. For correct access to the administration, the URL where OPTENET is installed must be added to the list of trusted sites on your browser. For example, if OPTENET is installed on http://192.168.0.240 and you are using Internet Explorer 6.0 you must access the menu Tools -> Internet Options -> Security -> Trusted sites and add the URL http://192.168.0.240.

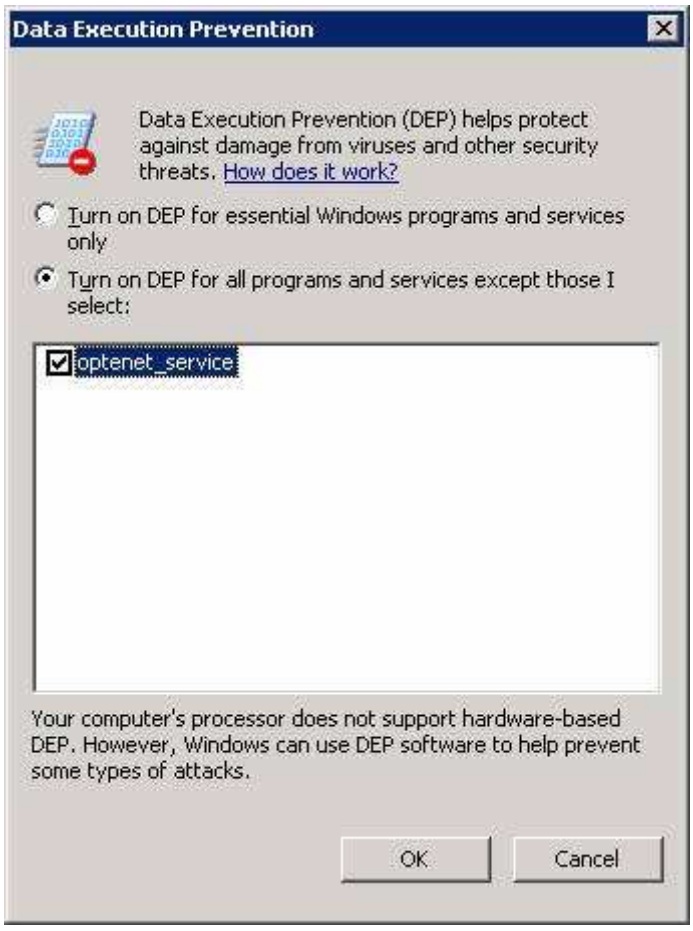


6.5. DEP closes OPTENET Server in W2003 SP1

Windows2003 SP1 provides the DEP tool. Under certain circumstances DEP may stop OPTENET Server and display the following message.

Data Execution Prevention - Microsoft Windows
To help protect your computer, Windows has closed this program.
Name: optenet_service
Change Settings
Close Message
Data Execution Prevention helps protect against damage from viruses or other threats. Some programs might not run correctly when it is turned on. For an updated version of this program, contact the publisher. What else should I do?

To solve this problem, right-click on 'My Computer' and select 'Properties. Then click on the 'Advanced Options' tab and then click on 'Configuration' in the 'Performance' group. Finally select the "Data Execution Prevention' tab and the following screen will display:


Data Execution Prevention
Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?
Turn on DEP for essential Windows programs and services only
Turn on DEP for all programs and services except those I select:
optenet_service
Your computer's processor does not support hardware-based DEP. However, Windows can use DEP software to help prevent some types of attacks.
OK
Cancel

Click on the second option; 'Turn on DEP for all programs and services except those I select'. Finally, select optenet_service from the list of services and programs and then click on 'OK'.

ANNEX

1. ADMINISTRATION OF OPTENET SERVER TROUGH A SECURE CONNECTION (ONLY LINUX ENVIRONMENT)

The OPTENET filter can be administered through a secure connection using the HTTPS protocol, by visiting this URL: https://host.domain from any browser. For this type of administration, the Stunnel programme must be running on the machine where the filter is installed. To access the web configuration in secure mode from Internet Explorer, you will need Stunnel version 3.22-1 or later. If Stunnel is not installed or if your version is earlier than 3.22-1, the steps for installation are:

- Copy the stunnel-3.22-1.i386.rpm package from the updates.redhat.com:/ 7.2/en/os/i386 ftp, accessing as an “anonymous user” on the machine where Stunnel is to be installed.

- Install the package. In the directory where the stunnel-3.22-1.i386.rpm file was copied, execute as root user:

  rpm -i stunnel-3.22-1.i386.rpm (Stunnel not installed)
  rpm -U stunnel-3.22-1.i386.rpm (Stunnel version earlier than 3.22-1)

- Check that installation was successful:

  rpm -qa | grep stunnel

  It should display:

  stunnel-3.22-1

- Generate the certificates file. In the /usr/share/ssl/certs directory, execute as root user:

  make stunnel.pem

  and enter the data requested.

- Edit the stunnelinit script, that is in the filter installation directory. Check the path of all the files that it refers to, taking into account the filter installation directory, and that the value of stunnel –r parameter is the port listening to the filter (10237). This script also sets the connection port with others machines, by default this port is 443 and therefore you can access the filter web administration by entering "https://host_ip".But if you choose set other port instead of the 443 you will have to type "https://host_ip: Port" in the browser. An other important point to indicate is that if you choose to set a port lower than 1024, i.e., 443 you will have to run the stunnel as a root.

- To run Stunnel, execute the stunnelinit script in the installation directory as root user:

  ./stunnelinit start

- To stop Stunnel, execute the stunnelinit script in the installation directory as root user:

  ./stunnelinit stop

When restarting or starting the filter, stunnel must also be restarted, but it is important to restart it after the filter is started, because when the filter is started it deletes all instances of stunnel that are running on the local machine.

If using multiple OPTENET Server installations with cluster management the OPTENET Server itself takes care of securing the communications.

2. ADMINISTRATION OF OPTENET VIA THE COMMAND LINE (OPTENET CLI V1.0)

2.1. Introduction

OPTENET CLI is an application that allows OPTENET Server to be administered via a command line. It is an alternative method of web administration, with the advantage that OPTENET CLI is capable of processing script files that contain multiple requests. Another characteristic of OPTENET CLI is that it allows any filter to be administered, simply by editing its configuration file.

OPTENET CLI provides an exhaustive control of everything that is typed into the command line in order to minimise errors. The OPTENET CLI command line interface is in English, but the user manual is available in various languages.

OPTENET CLI can be executed on the machine where OPTENET Server is running or on any other machine. You must keep in mind that if OPTENET CLI remotely administers a filter, it may not work correctly if it has to go through a proxy.

If using OPTENET CLI to modify the master server in a managed cluster you should note that all changes will be replicated in the slave servers.

The files that are going to be used by OPTENET CLI (the configuration file and script files) need to be in the directory where OPTENET CLI is being executed. Therefore, if OPTENET CLI is executed remotely, care must be taken to copy both files to the directory where it is being executed.

OPTENET CLI is installed in the tools subdirectory along with the configuration file cli.conf and the file script.txt, which can be modified to make multiple sequential changes. This file is empty by default.

2.2. Use

An explanation is provided below on how to use OPTENET CLI and make the most of the features that if offers.

2.2.1. Execution

In order to execute OPTENET CLI, go to the directory where it is installed and type in the following:

```
optenetcli
```

The OPTENET CLI welcome message will be displayed.

Now you are on the command line of OPTENET CLI, and the commands that you type in will be interpreted and executed.

2.2.2. Help

OPTENET CLI has a complete help system in text mode. To access it, type the following:

?

The names of all the OPTENET CLI commands will be displayed. Keep in mind that these are simply the names of the commands. Many of the commands have settings that must also be specified.

2.2.3. Commands

In order to find out the settings of a command, simply type in the name of a particular command, followed by a "?".

Example:
saveconfig ?

All of the OPTENET CLI commands are in one of the following formats:

- addxxxxxx
- savexxxxxx
- delxxxxxx
- sortxxxxxx

Where xxxxxx represents a chain of characters.
Example: saveconfig, delurlyes, sortrule...

Special care must be taken with characters in upper and lower case, given that OPTENET CLI makes a distinction between them. In other words, "saveconfig" does not mean the same thing as "SaveConfig."

In order to make handling OPTENET CLI simpler, all of the commands take lower case letters. Nevertheless, as it can be seen below, some of the settings have characters in upper case.

OPTENET CLI will display the list of available commands when you type in the following:

- ?
- A command that is not interpreted by OPTENET CLI.
- A valid command, but an incorrect number of settings.

When a command is typed with the correct number of settings, but one of the settings is incorrect, OPTENET CLI will show you how to use that command. Therefore, a logical process for executing a command would be the following:

- Type in "?" to see the available commands.
- Type in the name of the command selected from the list, followed by a question mark.

- Type in the name of the command followed by its settings as shown by OPTENET CLI.

If the command typed in is correct, and moreover it has been executed correctly, OPTENET CLI will display the following message:

Configuration added successfully

If the command typed in is correct, but it could not be executed, it will display the following message:

Error: Configuration could not be added

If the command entered does not exist, you will see the list of available commands. On the other hand, if the command exists, but the number of settings is incorrect, it will show you how to use that command.

If the command and the number of settings are correct, but one of the settings is incorrect, then you will see how to use that command, and it will show you the following message:

Error: Setting XX is not correct

Where XX refers to the setting number.

For some specific settings, a different message than the preceding one will be displayed. For example, if one of the settings is a day of the week and you type in “Fourteen,” OPTENET CLI will display the following:

Error: Fourteen is not a day of the week

Section 4 of this document provides a list of all valid commands. This section can be used as a quick reference guide.

2.2.4. Script file

In order for OPTENET CLI to execute all commands of a script file, simply type in the name of the script file with the txt extension.

Example: script.txt

OPTENET CLI will display the result of executing the requests as follows. If the request has been executed correctly:

Line XXX added successfully

Where XXX refers to the line number of the file.

If, on the other hand, a request is not correct, it will show you how to construct it correctly. Example:

USAGE: savekey PASSWORD
PASSWORD: Password for protecting sensitive information

It is important to keep in mind that the format of the requests of a script file is exactly the same as if it were typed in.

The format of a script file consists of having one single request per line. A clear and easily editable script file is thus obtained. Therefore, if two requests are written on the same line, OPTENET CLI will display an error on that line, and it will not be able to process either of the two requests.

2.2.5. Exit

In order to exit from OPTENET CLI, you must type in the following command:

exit

This command ends the execution of OPTENET CLI.

2.2.6. Configuration file

The OPTENET CLI configuration file is “cli.conf,” and it must be in the executable file directory. You can edit this file using any editor. The format is the following:

UserName
Password
Server IP
Server Port

As you can see, the file consists of only 4 lines, which allow you to select any OPTENET Server that is being executed in order to be able to administer it.

The first two lines are the username and the password that you need in order to administer OPTENET Server, which is the same one required in order to administer it through the web, for example. The default username and password are “optenet” and “12345678”.

The next two lines contain the necessary information for OPTENET CLI to know where to connect: the IP address of the machine where OPTENET Server is being executed and the port where it is listening. The default values for the IP is localhost (127.0.0.1) and for the WWW administration port 10237.

It is important to point out that the file must always have 4 lines and that they must be the aforementioned ones. If there is any line missing or there are too many lines in the file, or you attempt to insert various fields on a line, OPTENET CLI will return an error message when the configuration file is loaded.

2.3. Command references

This section shows a complete list of the commands with their respective settings, which the user can use as a quick reference guide. The commands are grouped together in sections in the same way as the buttons at the web site administrator.

2.3.1. Configuration

Within this option, we can configure the status of the filter, establish the blocking page or establish the directory where the logs are generated.

2.3.1.1. Saveconfig

All of the aforementioned characteristics are configured through a single command.

saveconfig FILTER_STATE URL_BLOCK LOGS_DIR FLAG1 BLOCKING_LOGS FLAG2 QUERY_LOGS CRYPT_STATUS
FILTER_STATE: "Active", "Inactive"
URL_BLOCK: Url indicating the blocking page
LOGS_DIR: Directory for logs output (local path)
FLAG1: "0", "1" (Disable/Enable Blocking_Logs)
BLOCKING_LOGS: IP USER DAY RULE CATEGORY FILETYPE URL
Each Value is:"0","1" Example: 0100110
FLAG2: "0", "1" (Disable/Enable Query_Logs)
QUERY_LOGS: IP CLIENT USER GROUP DAY URL TRAFFIC TIME ACCESSES RULE CATEGORY FILETYPE
Each Value is:"0","1" Example: 010011010011
CRYPT_STATUS: "0", "1" (Disable/Enable encryption of personal information in log files)

This is the format by which OPTENET CLI shows us how to use a command. “saveconfig” is the name of the command, and ‘FILTER_STATE’, ‘URL_BLOCK’ and ‘LOGS_DIR’ are the settings of this command.

If a setting can only take specific values, then those values are shown in quotation marks after the setting name. For example, in the case of “saveconfig”, FILTER_STATE can only take the values of “Active” or “Inactive.”

Note that both “Active” and “Inactive” have the first letter in upper case and the rest of the characters in lower case.

2.3.2. Authentication

In this section, OPTENET can be configured to explicitly authenticate users.

2.3.2.1. Saveauthen

saveauthen AUTHENTICATION SERVER TIME PORT
AUTHENTICATION: "1" (Active), "0" (Inactive)
SERVER: Server IP
TIME: Expiration time
PORT: Server port

2.3.3. LDAP Authentication

In this section, you can define new LDAP servers and modify or delete existing ones.

When authenticating users, the command in which the servers have been defined is followed.

2.3.3.1. Delauthencache

delauthencache

No settings are given to this command.

2.3.3.2. Sortldap

sortldap SORT LDAP_SERVER
SORT: "Up", "Down"
LDAP_SERVER: LDAP Server name

2.3.3.3. Delldap

delldap LDAP_SERVER
LDAP_SERVER: LDAP Server name

2.3.3.4. Saveldap

saveldap SERVER PORT BASE_TYPE ADMIN PASSWORD LDAP_SERVER (OLD_LDAP_SERVER)
SERVER: Server IP
PORT: Server port
BASE_TYPE: Base to search for users and groups
TYPE: "0"(Windows 2000) "1" (Lotus Domino) "2"(iPlanet)
ADMIN: Username to log on to server
Type if not administrator

PASSWORD: Password for username
Type if not administrator
LDAP_SERVER: Server name
OLD_LDAP_SERVER: Old server name
Use OLD_LDAP_SERVER when modifying server, not when creating

The last setting is given in brackets, which means that it is optional. In other words, this command can be used to make two different requests. If we do not specify the last setting, we will create a new LDAP server; and if we do specify the last setting, we will be modifying an existing LDAP server, whose name is specified by the last setting.

2.3.4. Urls classification

In this option, we can add URLs to the various categories by indicating if a particular URL belongs to a category or not.

2.3.4.1. Saveurlclas

saveurlclas URL CATEGORIES
URL: URL to be categorised
CATEGORY: An Optenet Server category
YES_NOT: "Yes" "Not"

2.3.4.2. Adduserurl

adduserurl CATEGORY LIST URL
CATEGORY: One of OPTENET Server categories
LIST: "Yes", "Not"
URL: The URL

2.3.4.3. Deluserurl

deluserurl CATEGORY LIST URL
CATEGORY: One of OPTENET Server categories
LIST: "Yes", "Not"
URL: The URL

2.3.5. Filtering rules

By using the filtering rules, we can easily personalise OPTENET Server in order to adapt it to the needs of our web.
In this option, you will be able to define these rules and all of their criteria: IP Groups, Users, User Groups, Categories, URLs, Files and Time Tables.

2.3.5.1. Addrule

Addrule

2.3.5.2. Sortrules

sortrules SORT RULE_NAME
SORT: "Up", "Down"
RULE_NAME: Name of the rule to be sorted

2.3.5.3. Delrule

delrule RULE_NAME
RULE_NAME: Name of the rule to be deleted

2.3.5.4. Renrule

renrule OLD_RULE_NAME NEW_RULE_NAME
OLD_RULE_NAME: Old name of the rule
NEW_RULE_NAME: New name of the rule

2.3.5.5. Addips

addips RULE_NAME FROM_IP TO_IP
RULE_NAME: Name of the rule
FROM_IP: First IP of IP range
TO_IP: Last IP of IP range

2.3.5.6. Delips

delips RULE_NAME FROM_IP TO_IP
RULE_NAME: Name of the rule

FROM_IP: First IP of IP range
TO_IP: Last IP of IP range

2.3.5.7. Savecat

savecat RULE_NAME CAT1 CAT2 ... CATN
RULE_NAME: Name of the rule
CAT1,...CATN: An Optenet Server category
Categories not written will be disabled

This command does not have a fixed number of settings, given that we can pass as many category names as required. The categories whose names are not passed as a setting will be deactivated, and those that are passed as a setting will be activated.

2.3.5.8. Addurlyes

addurlyes RULE_NAME URL_YES
RULE_NAME: Name of the rule
URL_YES: The URL to be added

2.3.5.9. Delurlyes

delurlyes RULE_NAME URL_YES
RULE_NAME: Name of the rule
URL_YES: The URL to be deleted

2.3.5.10. Adduser

adduser RULE_NAME USER
RULE_NAME: Name of the rule
USER: User affected by the rule

2.3.5.11. Deluser

del user RULE_NAME USER
RULE_NAME: Name of the rule
USER: User affected by the rule

2.3.5.12. Addhours

addhours RULE_NAME FIRST_HOUR LAST_HOUR FIRST_MINUTE LAST_MINUTE
RULE_NAME: Name of the rule
HOUR_INTERVAL: Hour range. Type XX:XX-XX:XX. Example: 08:30-19:37
Hours should be in range 0-59
Minutes should be in range 0-23

All of the settings of this command, except for the first, are integer parameters and are within a range. If characters or an integer out of range are entered, OPTENET CLI will return an error.

2.3.5.13. Delhours

delhours RULE_NAME HOUR_INTERVAL
RULE_NAME: Name of the rule

HOUR_INTERVAL: Time range (8:30-19:37)

The second setting is a time interval, and it is important to follow the format that is specified, i.e. XX:XX-XX:XX
If the time range is entered with another format, OPTENET CLI will return an error.

2.3.5.14. Saveday

saveday RULE_NAME DAY1 DAY2 ... DAY7
RULE_NAME: Name of the rule
DAY*: A valid day of the week
"Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday"

2.3.5.15. Addurlnot

addurlnot RULE_NAME URL_NOT
RULE_NAME: Name of the rule
URL_NOT: URL affected by the rule

2.3.5.16. Delurlnot

delurlnot RULE_NAME URL_NOT
RULE_NAME: Name of the rule
URL_NOT: URL affected by the rule

2.3.5.17. Savefile

savefile RULE_NAME FILE_TYPE1 FILE_TYPE2 ... FILE_TYPE7
RULE_NAME: Name of the rule
FILE_TYPE*: A valid file type (mp3, avi,...)

2.3.6. Updates

OPTENET Server periodically connects to the OPTENET web site in order to update its lists and in order to be able to filter the new categorised Internet addresses that arise every day. This option is used to define the update frequency of the lists.

2.3.6.1. Saveact

saveact FREQUENCY DAY_OF_WEEK DAY_OF_MONTH START_HOUR
END_HOUR TRY_INTERVAL PROXY_ADDR PORT PROXY
FREQUENCY: "Daily", "Weekly", "Monthly"
_OF_WEEK: "Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday",
"Saturday"
DAY_OF_MONTH: "1", "2", "...", "28"
START_HOUR: "0", "1", "...", "23"
END_HOUR: "1", "2", "...", "24"
TIME_INTERVAL: Time between attempts
PROXY_ADDR: Proxy address
PORT: Proxy port
PROXY: "0", "1"

Special care must be given to upper and lower case letters.

2.3.7. Administrator identification

In order to ensure the privacy of the configuration and administration, the web server requires the user to be authenticated, and it will therefore ask for the user name and the password. By default, the user name is **optenet** and the password is **12345678**. These values can be changed through web administration using the Administrator Identification option.

You should note that user creating and deleting depends on the permissions assigned. By default the Administrator (“optenet”, “12345678”) privileges are used; to change this edit the first two lines of cli.conf.

2.3.7.1. Addadmin

addadmin NEW_USER_NAME NEW_PASSWORD ENABLED PROFILE
NEW_USER_NAME: New user name
NEW_PASSWORD: New password for new user name
ENABLED: Profile enabled ("1") or disabled ("0")
PROFILE: "1" (Ordinary administrator)
"2" (Local administrator)
"3" (Urls administrator)
"4" (Reports administrator)
"5" (Sensitive information administrator)

2.3.7.2. Saveadmin

saveadmin OLD_USER_NAME NEW_USER_NAME NEW_PASSWORD ENABLED PROFILE
OLD_USER_NAME: Old user name
NEW_USER_NAME: New user name
NEW_PASSWORD: New password for new user name
ENABLED: Profile enabled ("1") or disabled ("0")
PROFILE: "1" (Ordinary administrator)
"2" (Local administrator)
"3" (Urls administrator)
"4" (Reports administrator)
"5" (Sensitive information administrator)

2.3.7.3. Deladmin

deladmin USER_NAME PROFILE
USER_NAME: Administrator user name
PROFILE: "1" (Ordinary administrator)
"2" (Local administrator)
"3" (Urls administrator)
"4" (Reports administrator)
"5" (Sensitive information administrator)

2.3.8. Working with cluster

OPTENET Server allows multiple instances of OPTENET Server to be managed that are being executed on different machines. We can create, edit, eliminate and connect to as many OPTENET Server instances as we wish.

2.3.8.1. Cluster

cluster FLAG
FLAG: "1" (Enable 'Cluster management')
"0" (Disable 'Cluster management')

2.3.8.2. Addcluster

addcluster CLUSTER_NAME
CLUSTER_NAME: Name of the new cluster

2.3.8.3. Savecluster

savecluster CLUSTER_NAME NEW_NAME
CLUSTER_NAME: Name of the cluster
NEW_NAME: New Name for the cluster

2.3.8.4. Delcluster

delcluster CLUSTER_NAME
CLUSTER_NAME: Name of the cluster

2.3.8.5. Addserver

addserver SERVER_NAME SERVER_IP SERVER_PORT HTTP_FLAG USERNAME PASSWORD CLUSTER_NAME
SERVER_NAME: Name of new server
SERVER_IP: Ip address of new server
SERVER_PORT: Port where server listens
HTTP_FLAG: "1" (Http), "0" (Https)
USERNAME: Username to log on to the server
PASSWORD: Password to log on to the server
CLUSTER_NAME: Server's cluster name

2.3.8.6. Saveserver

saveserver SERVER_NAME SERVER_OLD_NAME SERVER_IP SERVER_PORT HTTP_FLAG USERNAME PASSWORD CLUSTER_NAME
SERVER_NAME: New name for server
SERVER_OLD_NAME: Server old name
SERVER_IP: Ip address of server
SERVER_PORT: Port where the server listens
HTTP_FLAG: "1" (Http), "0" (Https)
USERNAME: Username to log on to the server
PASSWORD: Password to log on to the server
CLUSTER_NAME: Server's cluster name

2.3.8.7. Delserver

delserver SERVER_NAME CLUSTER_NAME
SERVER_NAME: Name of server
CLUSTER_NAME: Server's cluster name

2.3.9. Reports

OPTENET Server allows you to configure a reporting tool (OPTENET Reporter), which will receive the logs.

2.3.9.1. StoreReporter

storereporter REPORTER_IP REPORTER_PORT
REPORTER_IP: Ip address where OPTENET Reporter is currently running
REPORTER_PORT: Port number where OPTENET Reporter is currently listening

2.4. Most common problems

This section describes the most common problems and the way to solve them.

2.4.1. OPTENET CLI is not able start up

Check that the OPTENET CLI (optenetcli) executable file is in the current directory. Check that the configuration file (cli.conf) is also there.

2.4.2. An error message is displayed when a command is executed

If you receive an error message in one of the settings, check them one by one. Also check the lower and upper case letters of the command and its settings.

If the error refers to the fact that the configuration could not be added, first verify that OPTENET Server is being executed. Then check that the data in the configuration file (user, password, IP, port) is correct.
Finally, check that no proxy has been passed through in order to reach OPTENET Server.

2.4.3. A command is executed but the change is not reflected in OPTENET Server

If you execute an OPTENET CLI command and do not receive an error but rather a message stating that the configuration has been added, even though you check that the changes expected after executing that command have not occurred, then the problem resides in the fact that one of the settings refers to an element that does not exist.

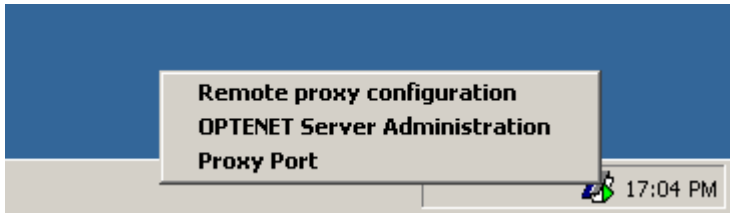
That element could be a rule, a category, a file type, a server or IP name, ...

3. OPTENET PROXY CONFIGURATION

The Optenet proxy has certain user configurable parameters such as the listening port, and the address of a secondary proxy if used for chaining.

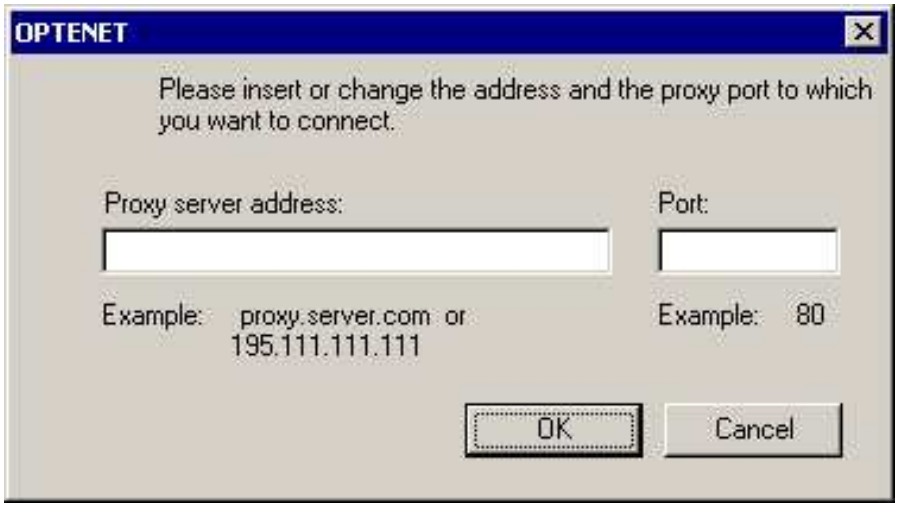
These options can be modified using the task bar icon:

Right clicking on the icon opens the following popup menu from which the required option can be selected:



3.1. Configuring a chained proxy (Configuration proxy)

If you want to configure a chained proxy the following window allows you to enter the data: the proxy IP and port.

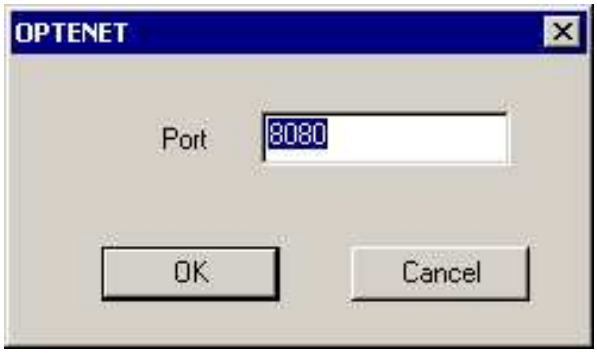


3.2. OPTENET Server administration

Click on this option and the OPTENET Server administration web page will open.

3.3. Port configuration (Port Proxy)

To modify the port the proxy uses to listen to user request on select this option and enter the new port:



4. DESCRIPTION OF OPTENET CATEGORIES

There follows a categorisation that OPTENET offers together with a brief description of them:

1. **Government:** Government, Local Authorities, State Administration...

2. **Anonymizers:** Web pages through which knowledge of the web addresses being accessed is prevented by third parties.

3. **Anorexia and Bulimia:** Sites encouraging anorexia and bulimia.

4. **Art:** Websites that provide information about the Arts: museums, sculpture, photography, literature, etc.

5. **Gambling:** Web pages of on-line casinos and bingos. It also includes gaming pages such as pools, lotteries etc.

6. **Banks and Financial Institutions:**

7. **Banners:** Advertisements inserted onto web pages, as well as the URLs of companies that are engaged in preparing these advertisements on the Web.

8. **Blogs:** Free pages where people can publish their diaries and any experiences, comments, ideas, etc. they wish to share over the Internet.

9. **Search engines:** Web pages used to search for other web addresses on the Internet, for example Google, Yahoo, Altavista, Alltheweb, etc.

10. **Chat:** Web sites that provide communication services (chat) with other users in real time.

11. **Malware:** Hardware, software or firmware which is intentionally entered onto a system for malicious or unauthorised purposes. A Trojan Horse is an example of malicious code.

12. **Bomb-making:** Web pages on how to make explosive.

13. **Shopping:** Web pages where goods and services may be bought.

14. **Web mail:** Web sites that provicde services for sending electronic mail.

15. **Sports:** Web pages with contents relating to teams and sports information.

16. **DNS Services:** this term covers connections from computers on the company's internal network to users' computers on the Internet, via http to a variable and configurable target port. This means that the company's Internet computer can make use of tools such as Remotely Anywhere which gives the user of the internal network complete control over the Internet computer and thus provides a way out by executing http, ftp, etc.

17. **Drugs:** Web pages with drug contents, both encouraging consumption and providing places and contacts to obtain them. Pages warning of their prejudicial effects are not included.

18. **Economy:** Web pages related to banks, stock exchanges, financial investments etc.

19. **Education:** Web pages related to primary and secondary schools, universities academies and courses in general.

20. **Employment:** Web pages related to situations vacant and wanted: It also includes head-hunters.

21. **Encounters:** Web pages through which you can meet other people: make friends, find a partner, etc.

22. **Leisure:** Web pages with information relating to films, theatre, books, restaurants, hobbies etc. Contents on how to spend spare time in general, except those contents included in chance, sport, games and travel, which have their own categories.

23. **Forum:** Forum.

24. **Guides:** websites that include city street maps, information about addresses, telephone numbers, etc.

25. **Hackers:** Web pages containing illegal software. Pages containing tools for pirating programs and documentation on how to avoid computer security measures in general.

26. **Hosting domains:** Websites of companies that host websites and from where Internet domains can be obtained.

27. **Info:** websites that provide generally useful information, such as the state of the roads, weather forecasts, etc.

28. **Computing:** Web pages with information related to hardware, software, Internet etc.

29. **Games:** Web pages where on-line games can be played or computer games downloaded.

30. **Legal:** websites containing information on legal matters.

31. **Logos/Ringtones:** Pictures or Songs (monophonic or polyphonic melodies) downloaded by mobile phone users.

32. **White list:** Web pages that do not belong to any kind of contents. The filtering rules that restrict the contents are not applied to them.

33. **Black list:** Web pages that are considered to belong to all the contents types. All the filtering rules restricting the contents are applied to them.

34. **Models:** Web pages where photos of models, both male and female, can be found. Pages where these types of photos show totally or partially nude models may be included in the pornography category.

35. **Music:** Web pages where music can be downloaded or bought. Sites with information related to singers and music groups in general.

36. **Pay-per-surf:** web pages which allow people to earn money on the Internet by receiving e-mails, surfing certain web pages, subscribing to free offers, etc.

37. **Personal websites:** Pages created on specialised hosting that are not included in other categories.

38. **Pornography:** Web pages with pornographic and erotic nature. It also includes access to sites for downloading where material of this type is found.

39. **Portals:** Web pages where you can find a wide range of contents: news, leisure, sports, games, music, etc.

40. **Press:** Web Pages of virtual newspapers and magazines.

41. **Racism:** Web pages of openly xenophobic content or that incite racist behaviour for religious, cultural, racist ideological etc motives.

42. **Remailers:** Web pages that readdress or transform other web pages.

43. **Society:** Web pages with contents related to celebrities. It also includes contents related to fashion, decoration aesthetics etc.

44. **Health:** Web pages wher you can find information (not scientific) about illnesses and their remedies.

45. **Sects:** Web pages with contents related to dangerous sects and that are universally accepted as such. Those that for reasons of different legislation from one country to another are considered sects in some and rightful religious associations in others are not included.

46. **Sexuality:** Articles about sex, adolescent sex, sex education etc., with no pornographic content.

47. **Instant Messenger Servers:** Sites where these programmes are registered to give the service and the pages related to them.

48. **P2P Servers:** Sites where these programmes are registered to give the service and the pages related to them.

49. **Spyware:** Pages that contain Spyware. Spyware is understood to mean software that compiles information from a computer and subsequently passes on this information to an external body without the knowledge or consent of the owner of the computer.

50. **Telecomunications:** Web pages which provide information about land-line services, mobile phones, Internet connections…

51. **Travel:** Travel agents' web pages and pages of tourist information, hotels. Lodging, methods of transport.

52. **Violence:** Web pages with contents of an openly violent nature or that incite to or defend violence.

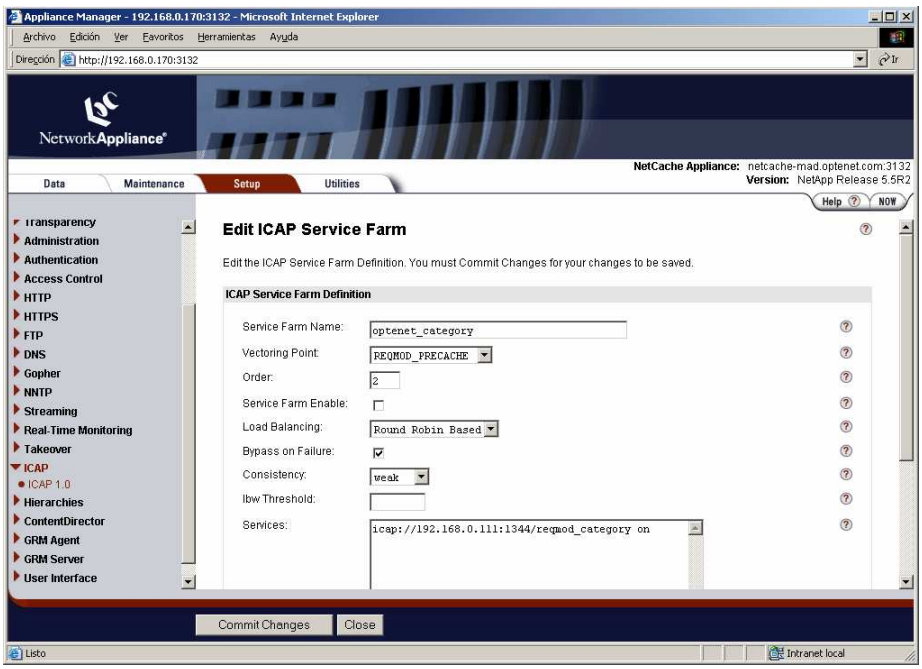
* On occasions a web page may belong to more than one category.

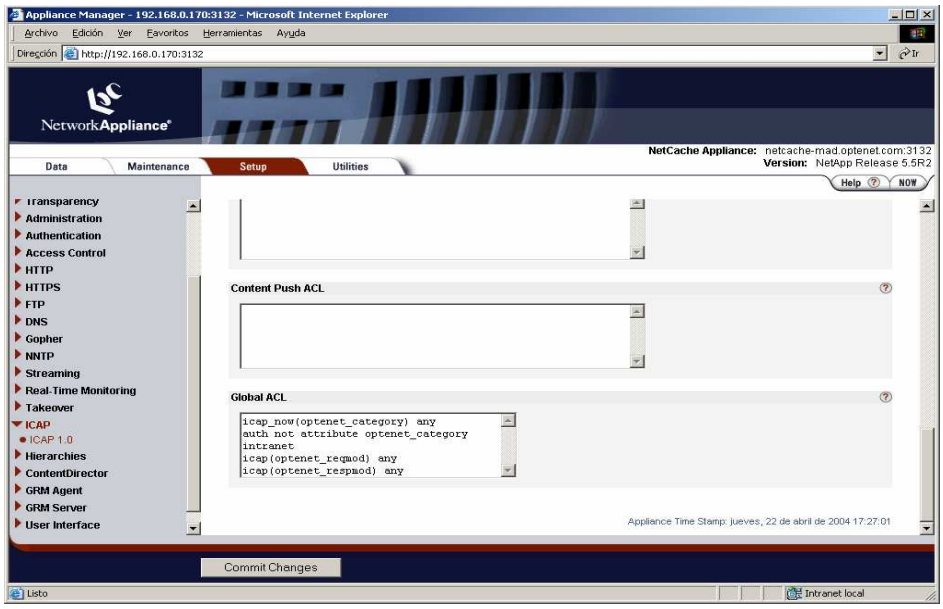
5. ICAP NOW

NetCache implements a different ICAP method called **icap now**. It is different from the normal icap methods in that the ICAP request is passed to the ICAP server – in this case OPTENET Server – even before carrying out user authentication. This can become useful if you want to carry out different operations depending on the result returned by the ICAP server, deciding, for example, only to ask users who are going to access certain categories for authentication.

OPTENET Server has implemented an ICAP service called reqmod_category, whose only mission is to categorize the accesses reaching it through that service. Unlike the other two services (reqmod_netcache and respmod_netcache) OPTENET Server does not block any access, it simply classifies them, returning the category to NetCache. To prevent an access being catalogued with more than one category, OPTENET Server uses the set-up file **etc/catpriority.txt** existing in its installation directory, so that, in the case of conflict between categories, the category that appears first in the file is assigned. Categories that do not appear are considered as having lower priority. If none of the possible categories is written (because both categories have been created by the administrator) the first one created in the system is chosen. You can edit catpriority.txt and order the categories as you wish. Once it has been saved, the filter must be restarted so the order takes effect. In addition, you can add new categories to the file, also modifying the first number that appears in the file, as this indicates the number of categories it has.

An example of a set-up for a NetCache in which the reqmod_category service has been defined to request authentication for all accesses not belonging to the Intranet category is shown below:





To be able to use this new service properly, you must indicate to OPTENET Server that it must launch more threads in order to handle requests for this new service. This is indicated in the Windows versions by modifying the registry key:
HKEY LOCAL MACHINE\SOFTWARE\OPTENET\OPTENET Server\IcapServices
Writing the value 3.
For Unix versions, you need to modify the script /usr/local/optenet/RunOPTENET adding the parameter **-icap_services 3**
In both cases you must restart the filter for the set-up to take effect.

6. SNMP MONITORING (ONLY LINUX ENVIRONMENT)

The filter can be monitored using the SNMP protocol, which can be easily integrated into the monitoring systems on the market.

For this purpose, the distribution of the filter includes an SNMP Agent, which acts as an entirely independent service, keeping the values of parameters up to date as regards the status of the filter in real time.

By default, the agent listens to port 161, although it can be configured to have a number of agents on the same machine.

The parameters that can be monitored are:

- Filter status: ENABLED / DISABLED /OFF.

(ID: .1.3.6.1.4.1.2021.254.1.0)

  - ENABLED: The filter is currently active.
  - DISABLED: The filter is on, but not active.
  - OFF: The filter is not running.

- Number of requests per second: X.

(ID: .1.3.6.1.4.1.2021.254.2.0.0)

- Number of blocks per second: X.

(ID: .1.3.6.1.4.1.2021.254.3.0.1849.0)

It also includes full information about the system, such as:

- System time/date.

(ID: .1.3.6.1.4.1.2021.4.0)

- Time the agent has been executed.

(ID: .1.3.6.1.2.1.1.3)

- Name of server.

(ID: .1.3.6.1.2.1.1.5)

6.1. Executing the SNMP agent

To activate the Optenet SNMP agent, you will need to execute this command:

optenet_snmp [–h] [–v] [–f] [–p PORT] [–l LOG_FILE]

- -h Displays the help in the command line
- -v Displays the product version
- -f It is not executed ion a child wire
- -p to establish a port other than 161 to listen to requests

-l to change the default log file (/usr/local/optenet/logs/optenet_snmp.log)

6.2. Automatic start

If you want the SNMP agent to start automatically with the filter, it will be necessary to edit the “RunOPTENET” and “filterinit” files, and remove the comments from the indicated lines, where the calls appear that are required to start and stop OptenetSnmp agent.

By default, in the start file the following appears as the port where the SNMP agent listens: **10237.**

6.3. Configuration of the agent

The agent needs a configuration file with the name: “snmp.conf”, with the following information:

Stat-url= 192.168.0.240 // URL or IP where the filter listens
Stat-port= 10234 // Port where the Web server of the filter listens (CGI statistics)

7. ADVANCED CGIS CONFIGURATION

Here the CGIs are described that the advanced filter configuration has implemented and that are only accessible by keying them in directly onto the browsers addess bars.

7.1. Reload

This option makes the filter re-read all the configuration files as web as the URL data base, A useful option if it is wished to clone the filter configuration of another server that has been recently incorporated to the cluster management of your organisation, without needing to stop and re-boot the filter. CAUTION. Use this option only in case of need, since the reloading of the database is costly in terms of CPU use.
To launch reload you must execute:

http://ip_del_filtro:10237/cgi-bin/ResetConf?

7.2. Dumping of Logs onto disks (/cgi-bin/FlushLogs)

This option means that the filter dumps the filter logs that it has on memory onto a disk. To optimise the yield, instead of writing its logs directly to disk every time it analyses a request, the filter uses a buffering system storing them on memory and dumping them onto disks when the buffers are full or every 5 minutes. This option causes the dumping of the logs that it has in its memory buffers at this moment. To launch the dumping of logs to disk, the following cgi must be executed:

http://ip del filtro:10237/cgi-bin/FlushLogs?LANG=eng

7.3. System information in text mode (/cgi-bin/sysinfotxt)

This option means that the filter returns the information of its status in text format instead of being a valid html page. It is very useful in unix installations where it is being administrated from command lines and the status of the filter needs to be seed since it may use the wget tool as in the following example:

Wget http://optuser:optpw@ip del filter:1037/cgi-bin/sysinfotxt?LANG=fra –O sysinfo.tx

8. CONFIGURING MICROSOFT ISA 2004

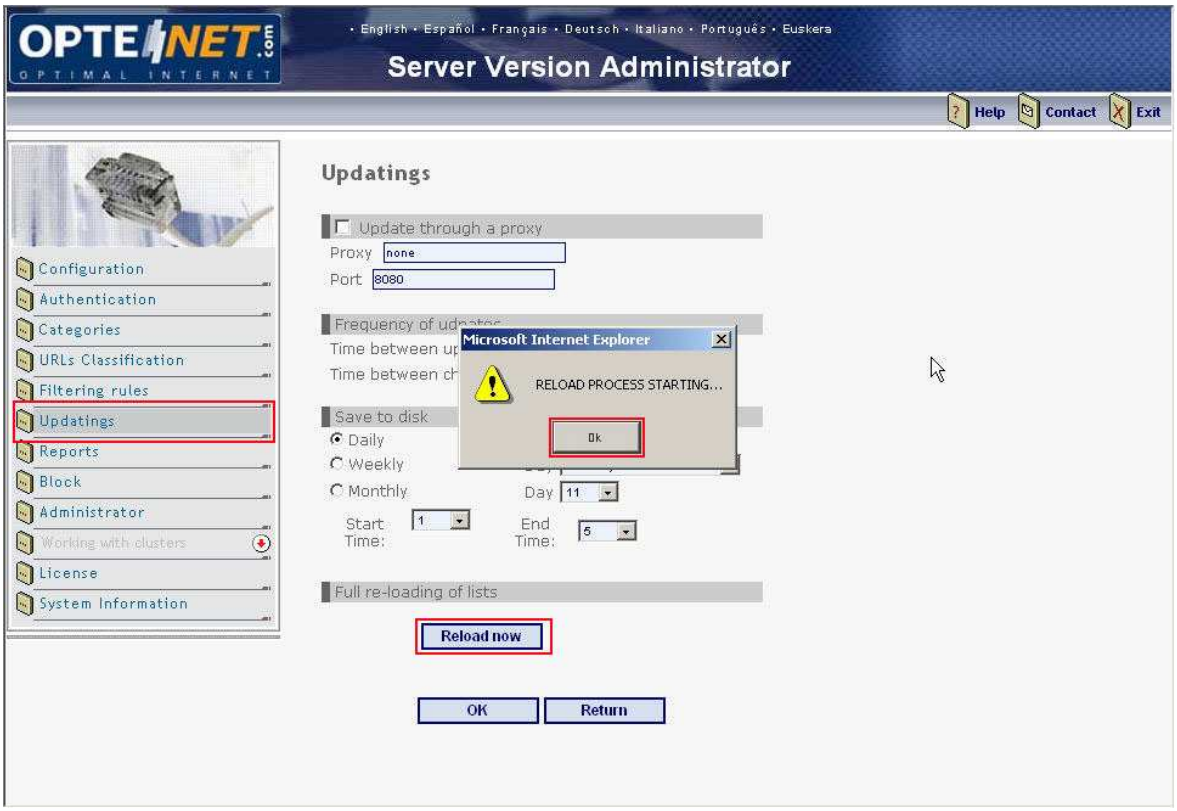
8.1. Introduction

Once the product has been installed on **MICROSOFT ISA SERVER 2004** (compatible from version 5.21.03 upwards), there is a series of functions which, by default, will not work because **MICROSOFT ISA SERVER 2004** is no longer merely a **PROXY,** but a **FIREWALL** with **PROXY** functions. For the product to function, we need to establish various rules in the configuration of **MICROSOFT ISA SERVER 2004**.

8.2. ACCESS TO OPTENET'S LICENCE AND UPDATES SERVERS

The default setting for the **MICROSOFT ISA SERVER 2004** is to have all accesses cut off, so if **OPTENET WEB FILTERING** attempts to connect to Optenet's licensing central (http://www.edunet.es) to learn the status of the licence it will warn us that it cannot access it by displaying the value "*Unknown*" in "*Licence status*".

In the same way, if we attempt to update the product database, either manually or via any of the automatic attempts made by the product, it will tell us that there is no access to the databases by displaying the value "*Error bringing in data*" in "*Total update status*".



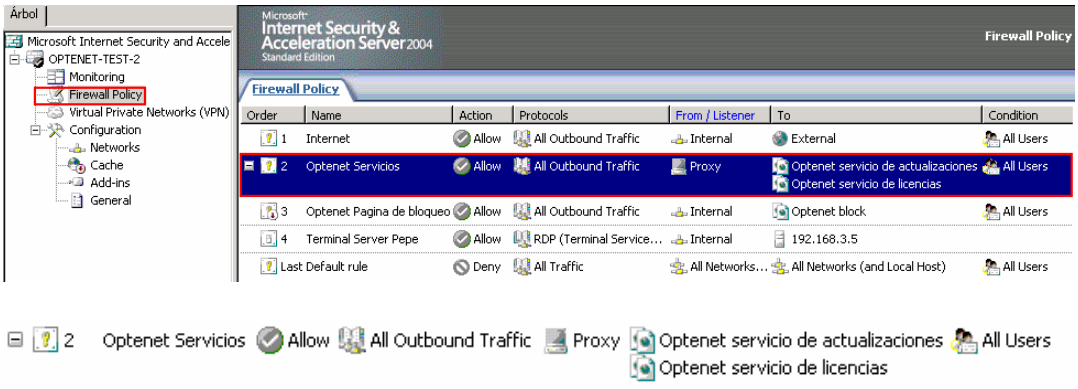
For the product to access the licensing central correctly, the MICROSFT ISA SERVER 2004 needs to be authorised for this address:

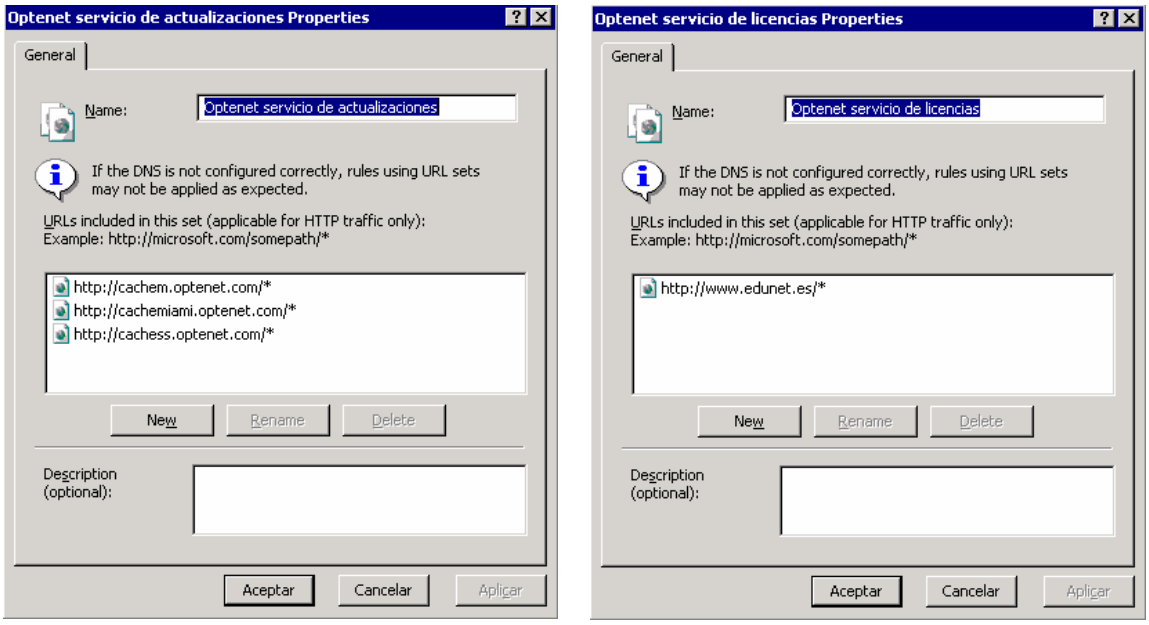
http://www.edunet.es/*

In the same way, for updating to occur correctly, the MICROSFT ISA SERVER 2004 needs to be authorised for the addresses of the OPTENET databases:

http://cachem.optenet.com/*
http://cachemiami.optenet.com/*
http://cachess.optenet.com/*

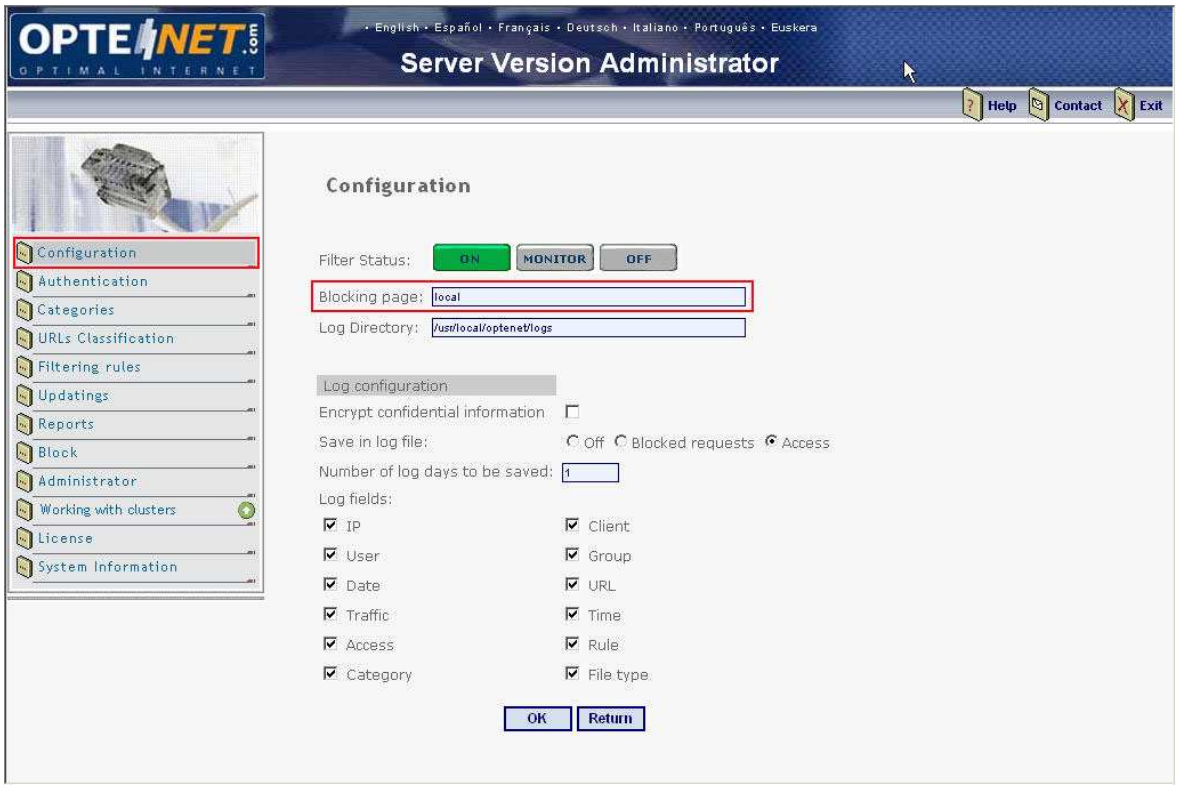
For this to occur, we create a rule which allows access to all these services from the MICROSOFT ISA SERVER 2004 server.


Árbol
Microsoft Internet Security and Accele
OPTENET-TEST-2
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004 Standard Edition
Firewall Policy
Firewall Policy
Order | Name | Action | Protocols | From / Listener | To | Condition
1 Internet Allow All Outbound Traffic Internal External All Users
2 Optenet Servicios Allow All Outbound Traffic Proxy Optenet servicio de actualizaciones, Optenet servicio de licencias All Users
3 Optenet Pagina de bloqueo Allow All Outbound Traffic Internal Optenet block All Users
4 Terminal Server Pepe Allow RDP (Terminal Service... Internal 192.168.3.5
Last Default rule Deny All Traffic All Networks... All Networks (and Local Host) All Users
2 Optenet Servicios Allow All Outbound Traffic Proxy Optenet servicio de actualizaciones, Optenet servicio de licencias All Users



8.3. ACCESS TO THE DEFAULT BLOCKING PAGE

The default setting for the MICROSOFT ISA SERVER 2004 is to have all accesses cut off, so if a client with permission to browse externally attempts to access an unauthorised page, it will be redirected to the default blocking page. This page is defined in the "*Configuration*" tab within OPTENET WEB FILTERING's web administration. The default value is "*local*".

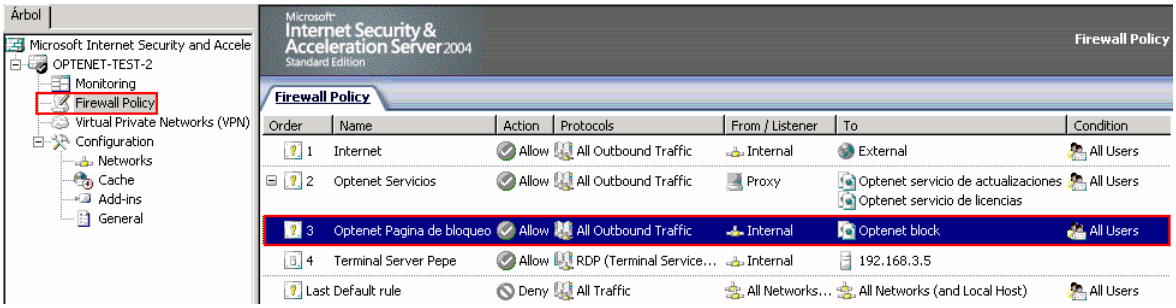


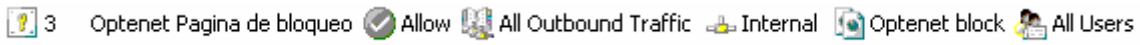
and this points at the MICROSOFT ISA SERVER 2004 server proper on port 10237 where OPTENET WEB FILTERING is hosting this page.

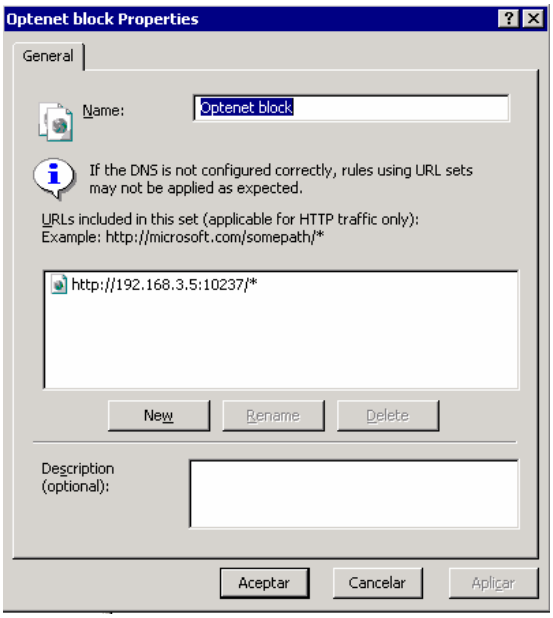
Because no rule has been defined to allow this port to be reached, requests for blocking will not display correctly, and a page like this one will display:

Direction
http://192.168.0.3:10237/cgi-bin/stop?CAT=[modelos-ac|pornografia-lg-au-ac]&RULE=[DenyPorn]&DATETIME=[09/Nov/2005:
Go
Network Access Message: The page cannot be displayed
Explanation: There is a problem with the page you are trying to reach and it cannot be displayed.
Try the following:
Refresh page: Search for the page again by clicking the Refresh button. The timeout may have occurred due to Internet congestion.
Check spelling: Check that you typed the Web page address correctly. The address may have been mistyped.
Access from a link: If there is a link to the page you are looking for, try accessing the page from that link.
If you are still not able to view the requested page, try contacting your administrator or Helpdesk.
Technical Information (for support personnel)
Error Code: 502 Proxy Error. The ISA Server denied the specified Uniform Resource Locator (URL). (12202)
IP Address: 192.168.3.5
Date: 25/11/2004 11:32:50
Server: optenet-test-2.maqueta.sytes.net
Source: proxy

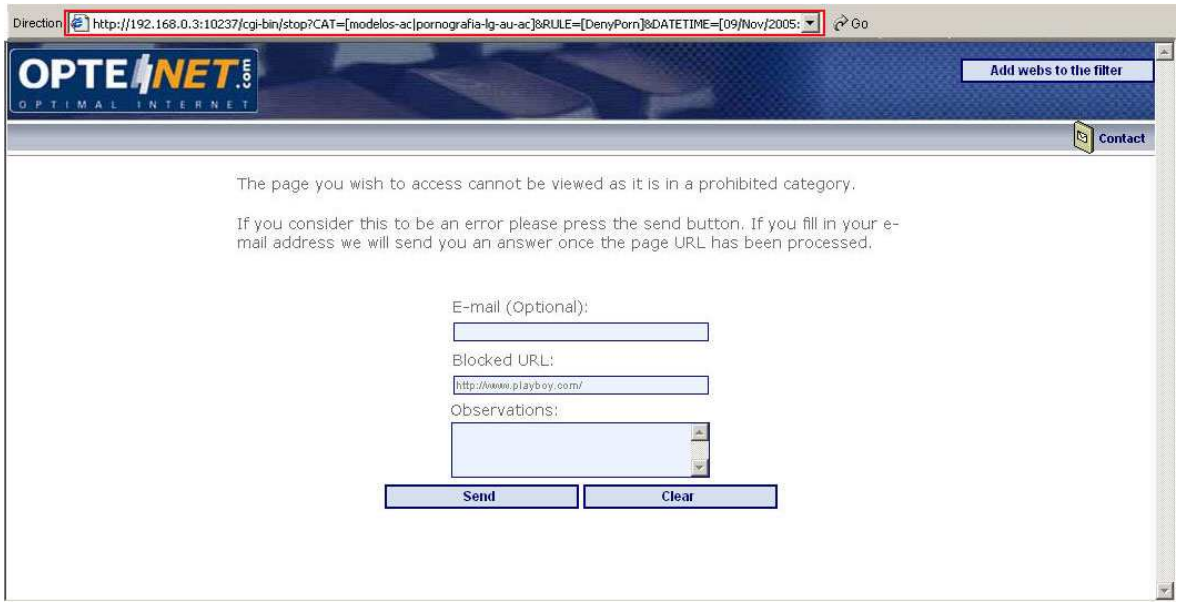
In order to prevent this occurring, we create a rule which allows all users with browsing rights to access port 10237 on the machine on which the MICROSOFT ISA SERVER 2004 server is installed.


Árbol
Microsoft Internet Security and Accele
OPTENET-TEST-2
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004
Standard Edition
Firewall Policy
Firewall Policy
Order
Name
Action
Protocols
From / Listener
To
Condition
1 Internet Allow All Outbound Traffic Internal External All Users
2 Optenet Servicios Allow All Outbound Traffic Proxy Optenet servicio de actualizaciones Optenet servicio de licencias All Users
3 Optenet Pagina de bloqueo Allow All Outbound Traffic Internal Optenet block All Users
4 Terminal Server Pepe Allow RDP (Terminal Service... Internal 192.168.3.5
Last Default rule Deny All Traffic All Networks... All Networks (and Local Host) All Users





Thus we can be blocked and reach the correct blocking page.


Direction
http://192.168.0.3:10237/cgi-bin/stop?CAT=[modelos-ac|pornografia-lg-au-ac]&RULE=[DenyPorn]&DATETIME=[09/Nov/2005:
Go
OPTENET.com
OPTIMAL INTERNET
Add webs to the filter
Contact
The page you wish to access cannot be viewed as it is in a prohibited category.
If you consider this to be an error please press the send button. If you fill in your e-mail address we will send you an answer once the page URL has been processed.
E-mail (Optional):
Blocked URL:
http://www.playboy.com/
Observations:
Send
Clear